Configure Local Web Authentication with External Authentication

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Web Authentication

- Types of Authentication
- Database for Authentication

Local Web Authentication

Local Web Authentication with External Authentication

Configure

- Network Diagram

Configure Local Web Authentication with External Authentication on the CLI

- Configure AAA Server and Server Group
- Configure Local Authentication and Authorization
- Configure Parameter Maps
- Configure WLAN Security Parameters
- Create Wireless Policy Profile
- Create a Policy Tag
- Assign a Policy Tag to an AP

Configure Local Web Authentication with External Authentication on the WebUI

- AAA Configuration on 9800 WLC
- WebAuth Configuration
- WLAN Configuration
- Policy Profile Configuration
- Policy Tag Configuration
- Policy Tag Assignment

ISE Configuration

Connect Guest Client

Verify

- Show WLAN Summary
- Show Parameter Map Configuration
- Show AAA Information

Troubleshoot

- Common Issues
- Conditional Debug and Radio Active Trace and Embedded Packet Capture
- Example of a Successful Attempt

Related Information

Introduction

This document describes how to configure Local Web Authentication with External Authentication on a 9800 WLC and ISE.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 9800 Wireless LAN Controllers (WLC) configuration
- Lightweight Access Points (LAPs)
- How to set up and configure an external web server Identity Services Engine (ISE).
- How to set up and configure DHCP and DNS servers.

Components Used

The information in this document is based on these software and hardware versions:

- 9800-40 WLC Cisco IOS® XE, Version 17.18.4a with APSP1 and APSP2
- Identity Services Engine (ISE), Version 3.2.0.542
- Cisco® Wireless 9172I Series Wi-Fi 7 Access Point, Version 17.18.4.202

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Web Authentication

Web authentication is a Layer 3 security feature that allows guest users to have access to the network.

This feature is designed to provide easy and secure guest access to open SSIDs, without the need to configure a user profile, and it can also work with Layer 2 security methods.

The purpose of web authentication is to allow untrusted devices (guests) to access the network with limited network access privileges, through a guest WLAN that can be configured with security mechanisms, and the security of the network not compromised. For the guest users to have access to the network, they need to authenticate successfully, that is, they need to provide the correct credentials or accept the Acceptable Use Policy (AUP) to gain access to the network.

Web authentication is a benefit for companies because it drives user loyalty, makes the company compliant to use a disclaimer that the guest user must accept, and allows the company to engage with visitors.

To deploy web authentication, it must be taken in consideration how the guest portal and authentication are handled. There are two common methods:

- Local web authentication (LWA): A method of redirection of guest users to a portal directly from the WLC. The redirection and pre-WebAuth ACL are locally configured on the WLC.
- Central web authentication (CWA): A method of redirection of guest users where the redirection URL and the redirect ACL are centrally configured on an external server (for example ISE) and communicated to the WLC via RADIUS. In central web authentication the redirect URL and redirect ACL are centrally located on an external server (such as RADIUS). The RADIUS server is the one that handles the authentication, it sends instructions to the WLC. In CWA, the WLC does not require a local web-auth certificate, only one certificate is needed on the central web portal, and requires a central authentication server, such as ISE. To read CWA in more detail navigate to Configure Central Web Authentication (CWA) on Catalyst 9800 WLC and ISE.

In Local Web Authentication, the web portal can be present on the WLC or on an external server. In LWA with External Authentication, the web portal is present on the WLC. In LWA with External Web Server, the web portal is present on an external server (such as Cisco DNA Spaces). An example of LWA with External Web Server is described in detail at: Configure DNA Spaces Captive Portal with Catalyst 9800 WLC.

Diagram of the different web authentication methods:

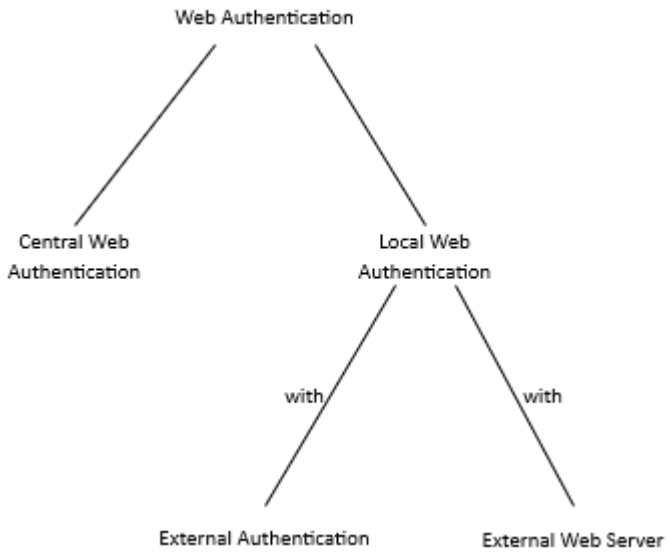


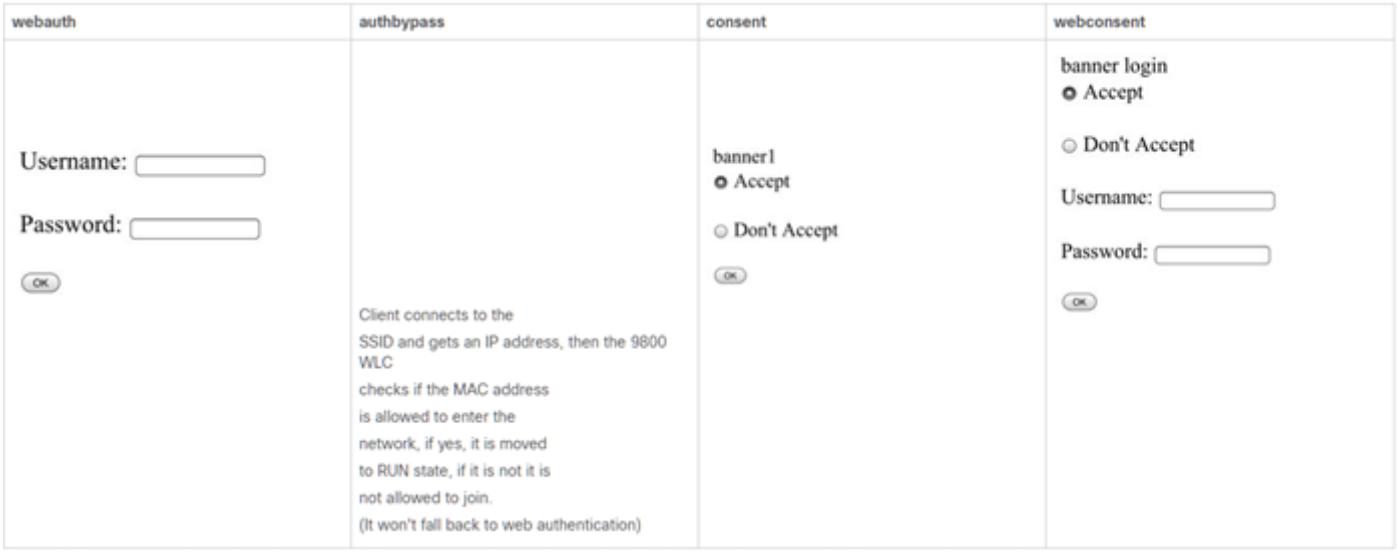
Diagram of the Different Web Authentication Methods

Note: If you are deploying Wi-Fi 7 APs with web authentication on a 9800 WLC, ensure you are running a recommended Cisco IOS XE release such as 17.18.4a or later.

Types of Authentication

There are four types of authentication to authenticate the guest user:

- Webauth: Enter username and password.
- Consent (web-passthrough): Accept AUP.
- Authbypass: Authentication based on the MAC address of the guest user device.
- Webconsent: A mix between username/password and accept AUP.



Four Types of Authentication to Authenticate the Guest User

Database for Authentication

The credentials for authentication can be store on an LDAP server, locally on the WLC or on the RADIUS server.

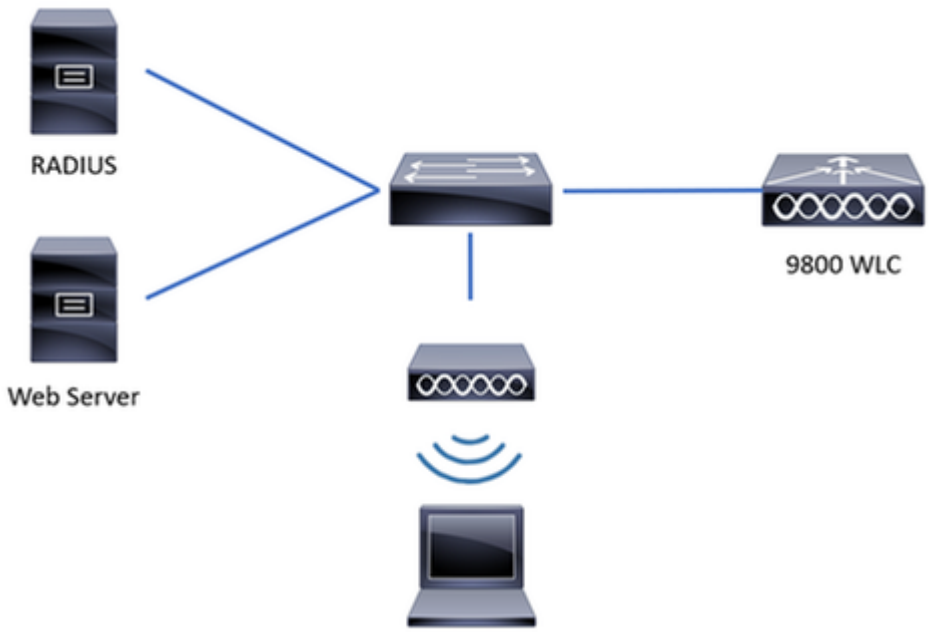
- Local database: The credentials (username and password) are stored locally on the WLC.
- LDAP database: The credentials are stored in the LDAP back-end database. The WLC queries the LDAP server for the credentials of a particular user in the database.
- RADIUS database: The credentials are stored at the RADIUS back-end database. The WLC queries the RADIUS server for credentials of a particular user in the database.

Local Web Authentication

In local web authentication the guest user is redirected to a web portal directly from the WLC.

The web portal can be in the WLC or in another server. What it makes local is the fact that the redirect URL and the ACL that matches traffic must be on the WLC (not the location of the web portal). In LWA, when a guest user connects to the guest WLAN, the WLC intercepts the connection from the guest user and redirects them to the web portal URL, where the guest user is asked to authenticate. When the guest user enters credentials (username and password), the WLC captures the credentials. The WLC authenticates the guest user with a LDAP server, RADIUS server or local database (database present locally on the WLC). In case of RADIUS server (an external server such as ISE), it can be used not also to store credentials, but also to provide options for device registration and self-provisioning. In case of an external web server, such as Cisco DNA Spaces, the web portal is present there. In LWA there is one certificate on the WLC and another on the web portal.

The image represents the generic topology of LWA:



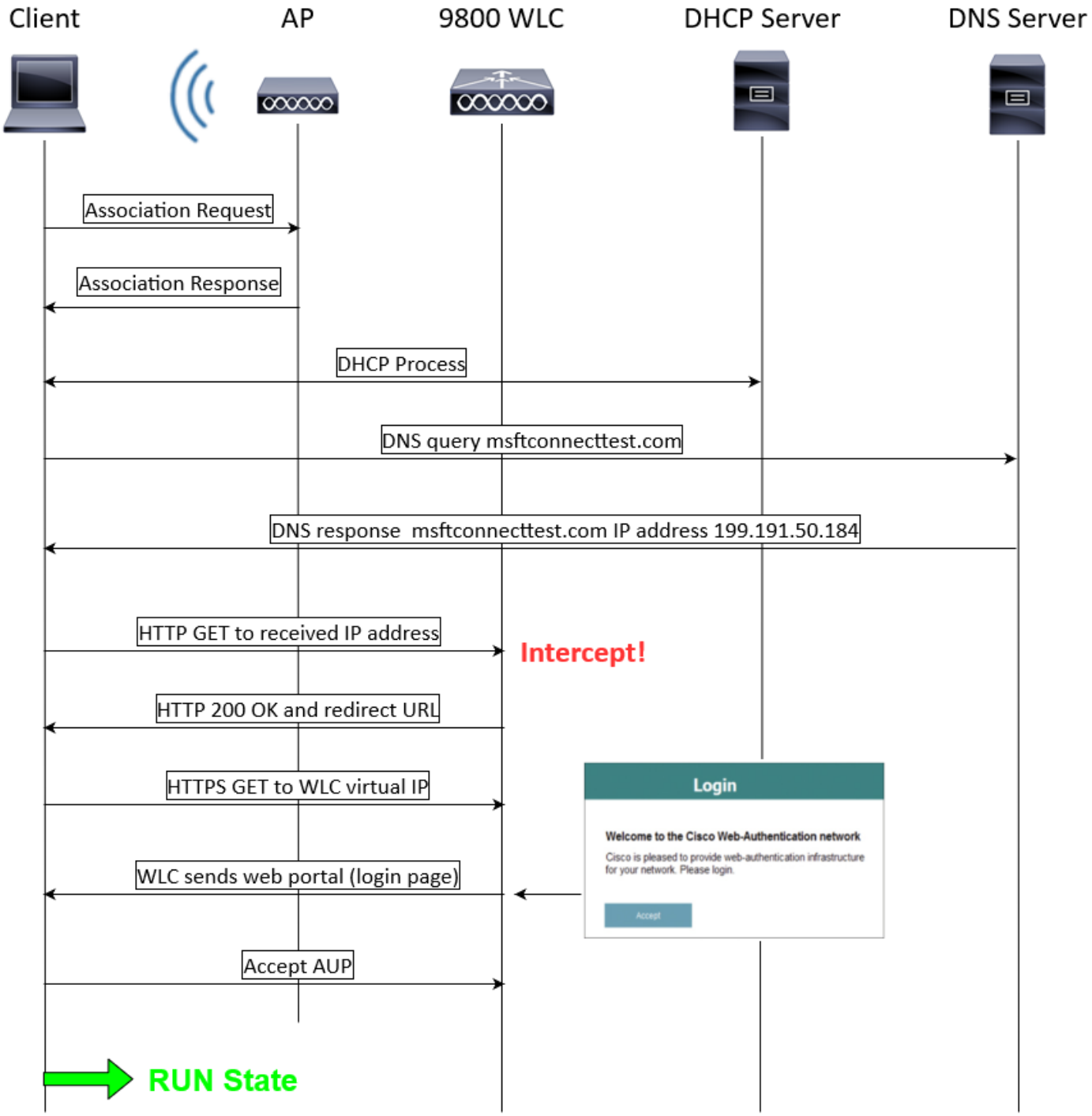
Generic Topology of LWA

Devices in the network topology of LWA:

- Client: Sends requests to DHCP and DNS server, requests access to the guest WLAN, and responds to requests from the WLC.
- Access Point: Connected to a switch, broadcasts the guest WLAN, and provides wireless connection to guest users devices. It also allows DHCP and DNS packets before the guest user is authenticated (before enter valid credentials).
- WLC: Manages the APs and clients. The WLC hosts the redirect URL and the ACL that matches traffic. Intercepts HTTP requests from the guest users, redirects them to an web portal (log in page) where guest users have to authenticate. It captures the credentials and authenticates the guest users, and it sends access requests to an external server, LDAP server or local database to confirm if the credentials are valid.
- Authentication server: Responds to access requests from the WLC with access accept/reject. The authentication server validate the credentials from the guest user and notifies the WLC if the credentials are valid or not valid. If credentials are valid, the guest user is authorized to access the network (the authentication server provides options for device registration and self-provisioning). If credentials are not valid, the guest user is denied access to the network.

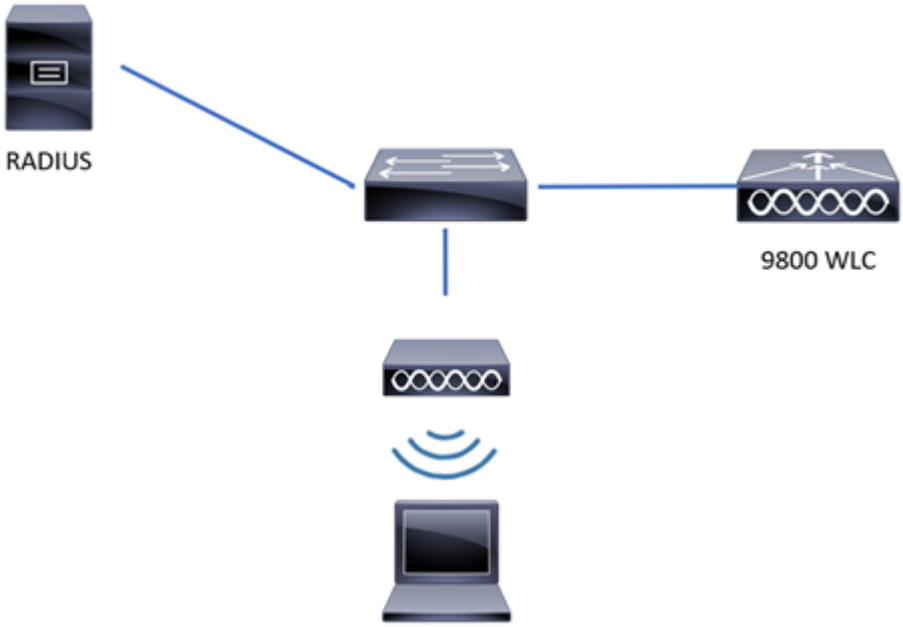
LWA flow:

- The guest user associates with an AP that broadcasts the guest WLAN.
- The guest user goes through the DHCP process in order to get an IP address.
- The guest user wants to make an internet connectivity check to the captive portal. If it is an Apple device, it tries the Apple captive portal; if it is an Android device it tries the Android captive portal; if it is a Windows device it tries the Windows connect test portal.
- The guest user sends a DNS query to ask for the captive portal IP address. The DNS server responds to the query with the correspondent IP address.
- The guest user sends an HTTP GET message to the IP address of the captive portal.
- The WLC intercepts that message and replies to the guest user with HTTP 200 OK and the redirect URL.
- The guest user sends a HTTPS GET message to the WLC virtual IP and the WLC responds with the web portal.
- The guest user is asked to enter authentication credentials on the web portal.
- The web portal redirects the user back to the WLC with the provided credentials (if an external web portal is used).
- The WLC authenticates the guest user through a local database, or it sends a query to the RADIUS or LDAP server, to confirm if the credentials are correct (if the authentication type is webconsent or webauth).
- If the credentials are correct, the WLC authenticates the guest user and it goes to RUN state. If credentials are wrong, the WLC deletes the guest user.
- The WLC redirects the client back to the original URL that was entered in the web browser.



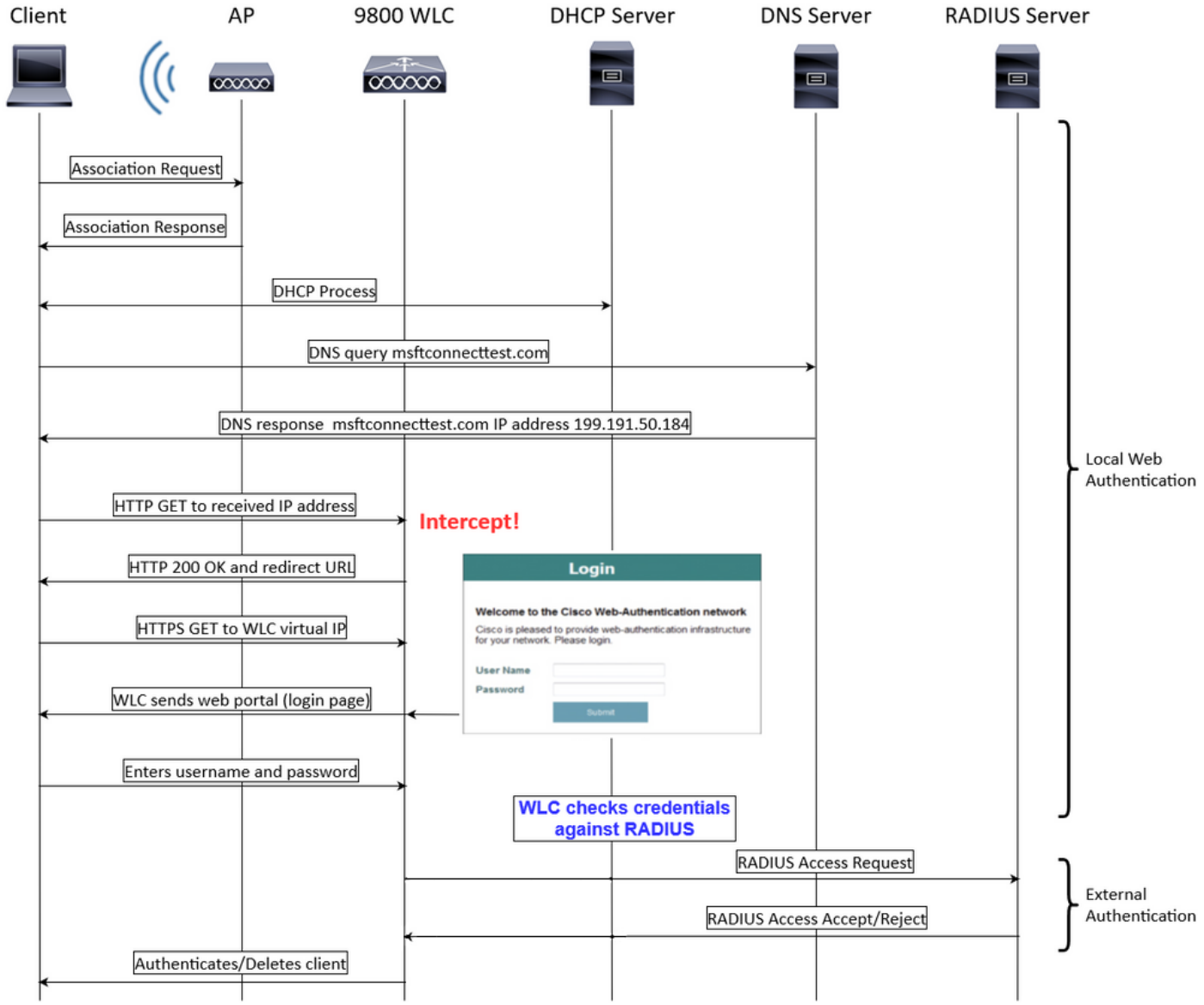
LWA Flow

Local Web Authentication with External Authentication



Generic Topology of LWA-EA

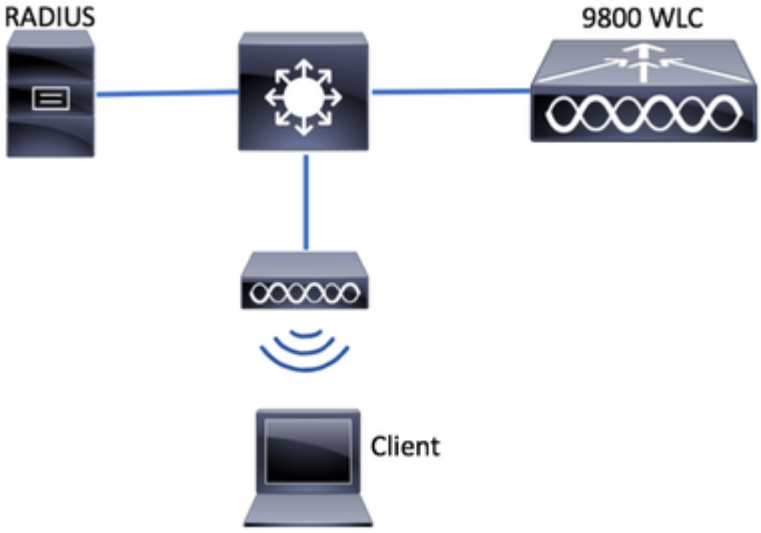
LWA-EA is a method of LWA where the web portal and redirection URL are located on the WLC and the credentials are stored on an external server, such as ISE. The WLC captures the credentials and authenticates the client through an external RADIUS server. When guest user enters credentials, the WLC checks the credentials against RADIUS, it sends a RADIUS Access Request and receives a RADIUS Access Accept/Reject from the RADIUS server. Then, if the credentials are correct, the guest user goes to RUN state. If the credentials are incorrect, the guest user is deleted by the WLC.



LWA-EA Flow

Configure

Network Diagram



Network Diagram

Note: This configuration example only covers central switching/authentication. The flex local switching configuration have slight different requirements for to configure web authentication.

Configure Local Web Authentication with External Authentication on the CLI

Configure AAA Server and Server Group

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#radius server RADIUS
9800WLC(config-radius-server)#address ipv4 <ip address> auth-port 1812 acct-port 1813
9800WLC(config-radius-server)#key cisco
9800WLC(config-radius-server)#exit
9800WLC(config)#aaa group server radius RADIUSGROUP
9800WLC(config-sg-radius)#server name RADIUS
9800WLC(config-sg-radius)#end
```

Configure Local Authentication and Authorization

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION group RADIUSGROUP
9800WLC(config)#aaa authorization network LWA_AUTHORIZATION group RADIUSGROUP
9800WLC(config)#end
```

Configure Parameter Maps

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)# parameter-map type webauth global
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint <trustpoint name>
9800WLC(config-params-parameter-map)#end
```

Configure WLAN Security Parameters

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wlan LWA_EA 1 LWA_EA
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

Create Wireless Policy Profile

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless profile policy POLICY_PROFILE
9800WLC(config-wireless-policy)#vlan <vlan name>
9800WLC(config-wireless-policy)#no shutdown
9800WLC(config-wireless-policy)#end
```

Create a Policy Tag

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless tag policy POLICY_TAG
9800WLC(config-policy-tag)#wlan LWA_EA policy POLICY_PROFILE
9800WLC(config-policy-tag)# end
```

Assign a Policy Tag to an AP

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#ap <MAC address>
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
9800WLC(config-ap-tag)#end
```

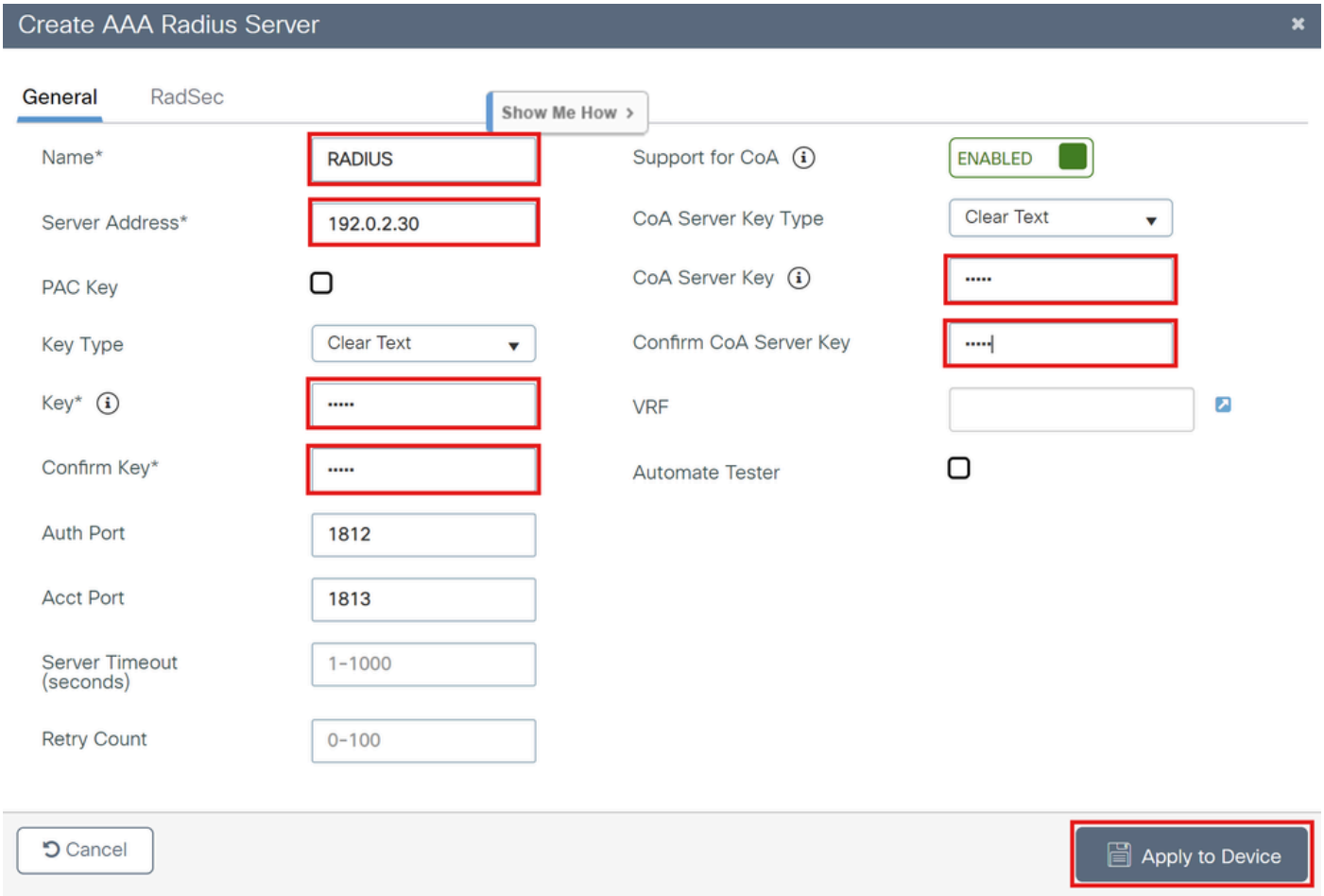
To finish the configuration on the ISE side, please jump to the *ISE Configuration* section.

Configure Local Web Authentication with External Authentication on the WebUI

AAA Configuration on 9800 WLC

Step 1. Add the ISE server to the 9800 WLC configuration.

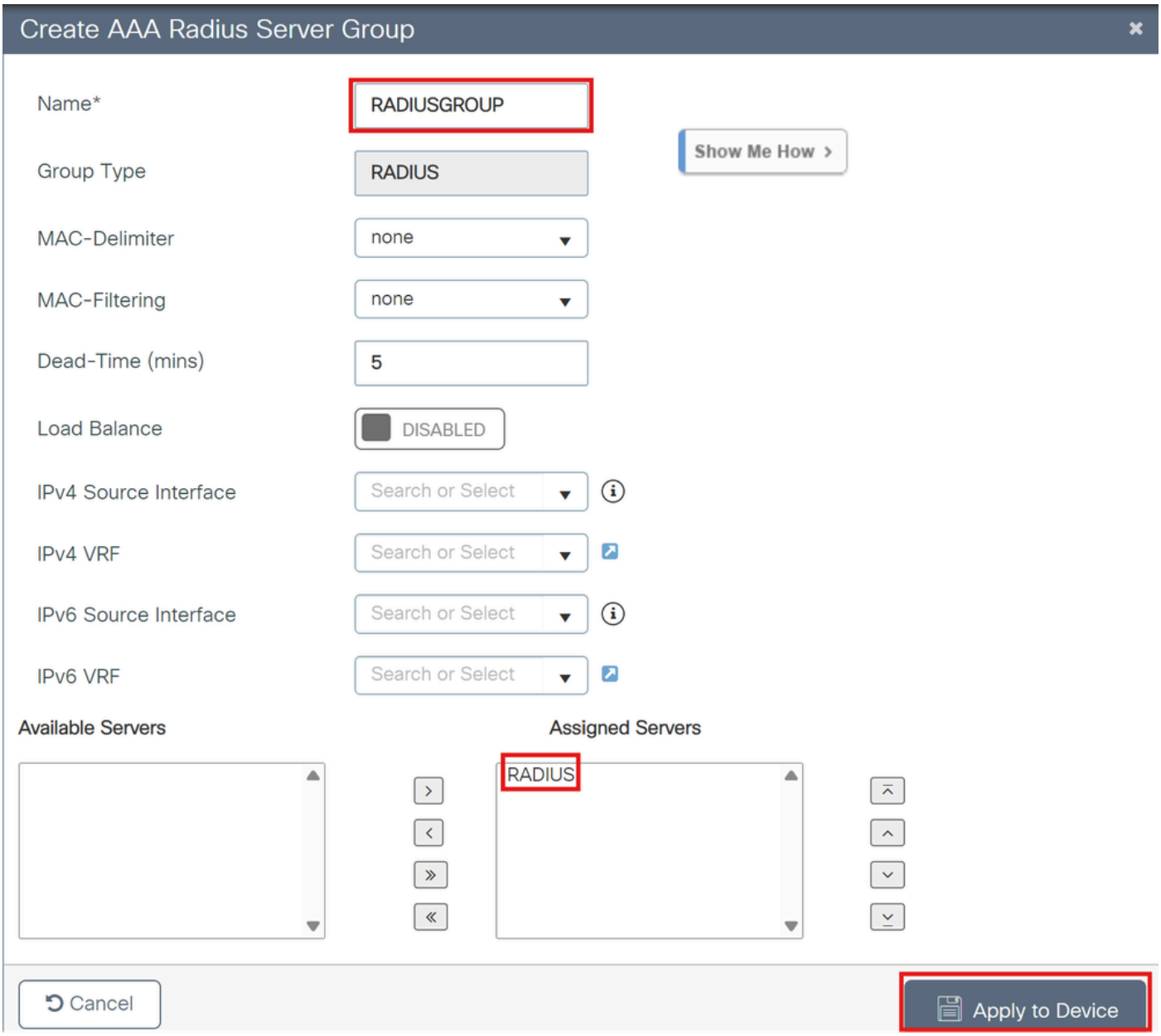
Navigate to **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add** and enter the RADIUS server information as shown in the image:



AAA Configuration on 9800 WLC

Step 2. Add the RADIUS server group.

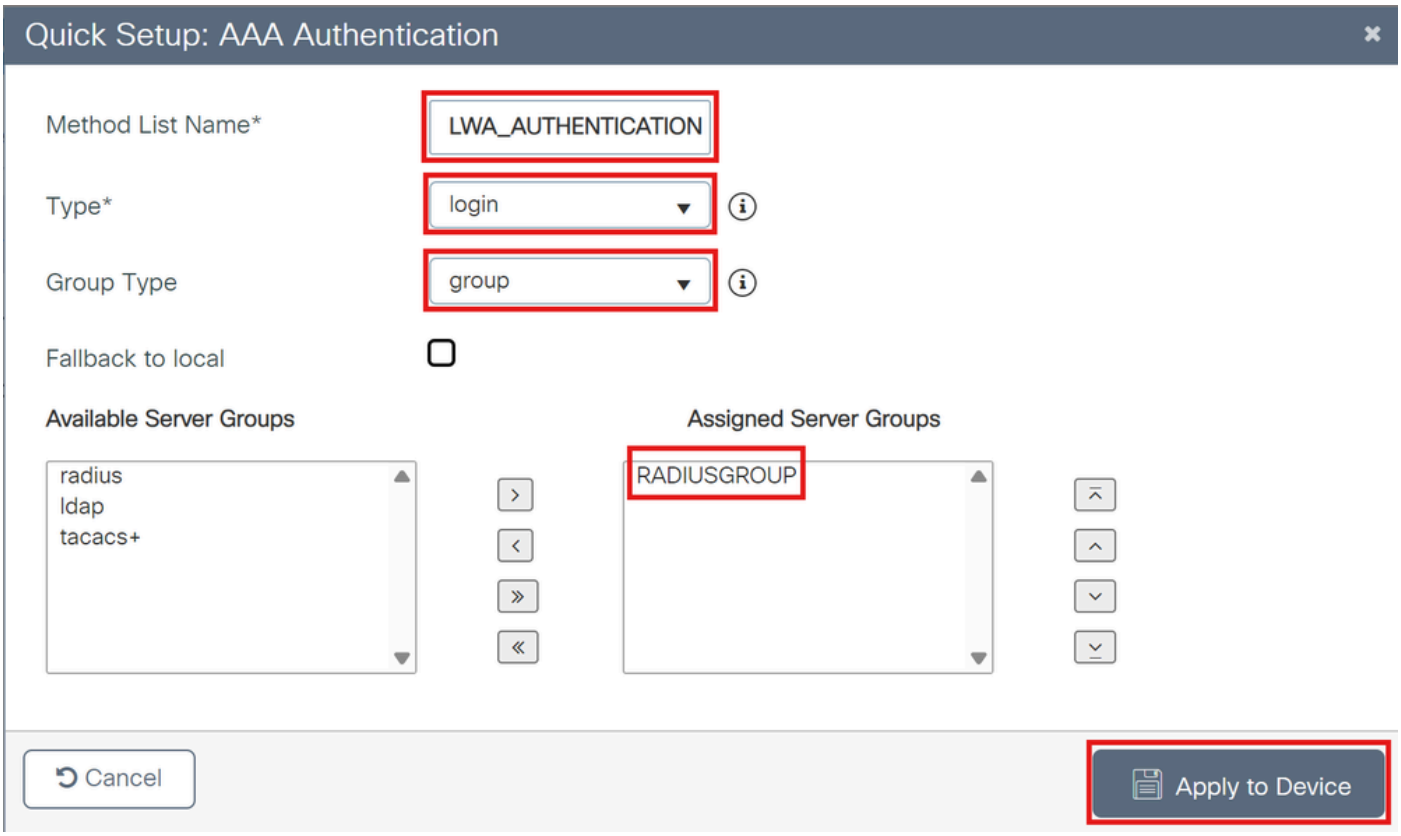
Navigate to **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers Group > + Add** and enter the RADIUS server group information:



Add the RADIUS Server Group

Step 3. Create an authentication method list.

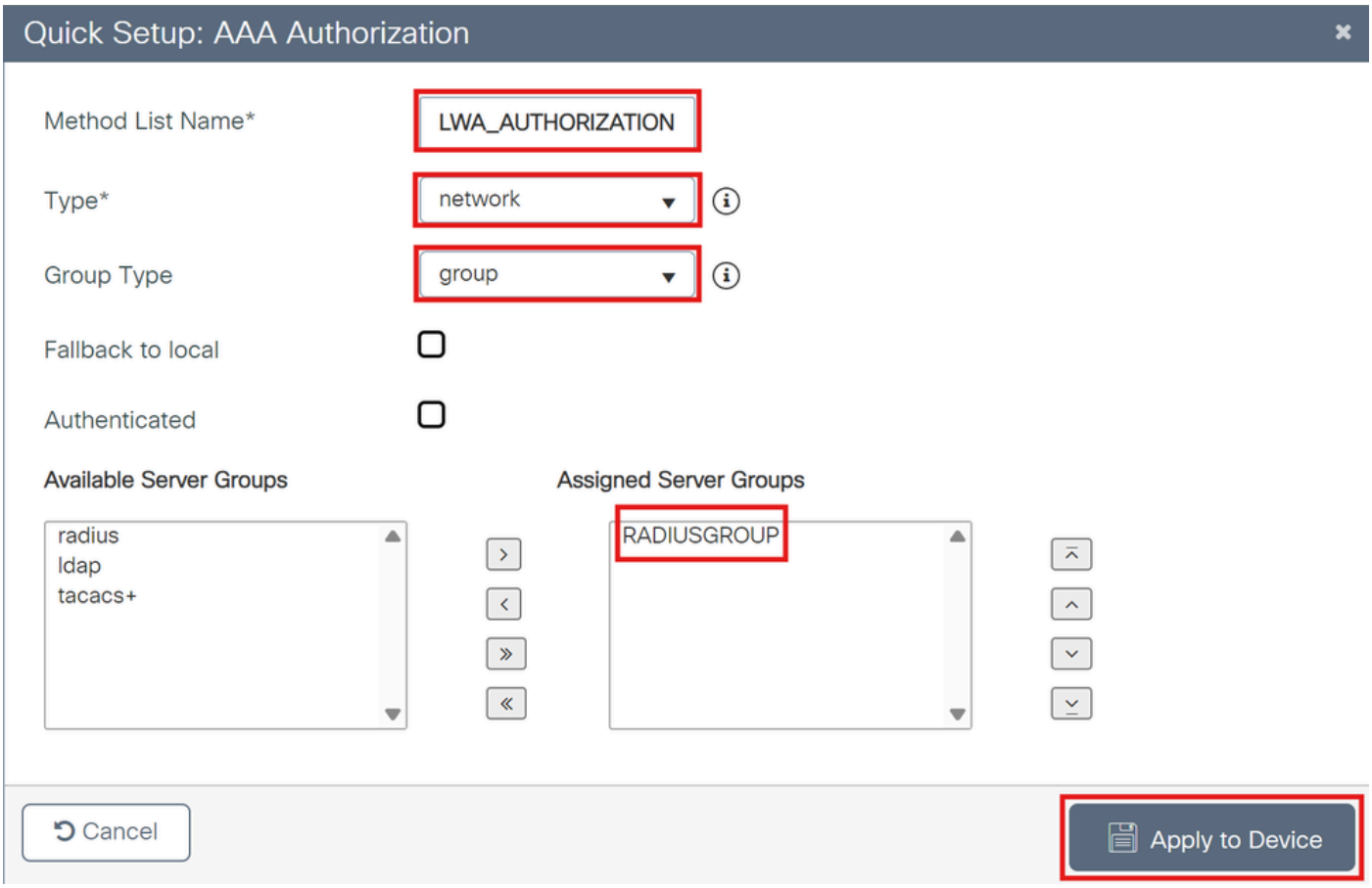
Navigate to **Configuration > Security > AAA > AAA Method List > Authentication > + Add:**



Create an Authentication Method List

Step 4. Create an authorization method list.

Navigate to **Configuration > Security > AAA > AAA Method List > Authorization > + Add**:

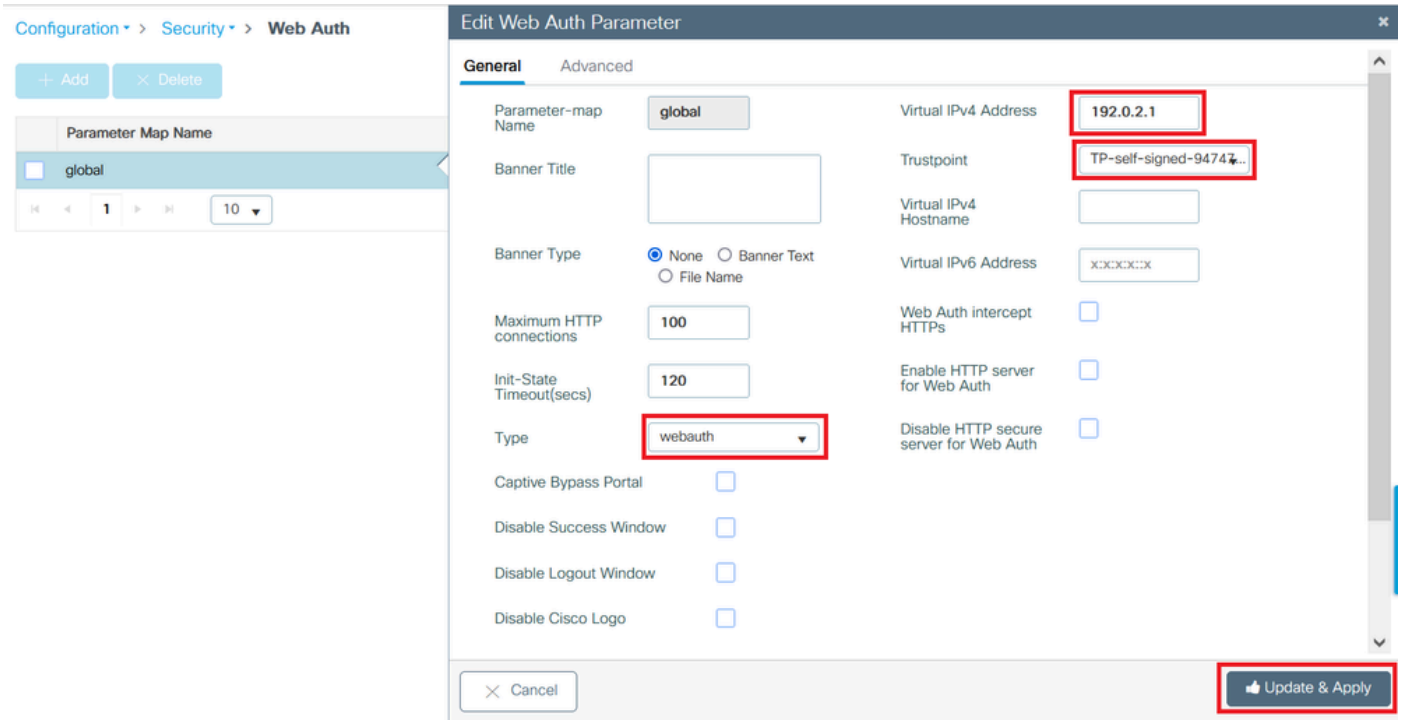


Create an Authorization Method List

WebAuth Configuration

Create or edit a parameter map. Select the type as **webauth**, the **Virtual IPv4 Address** must be an address not used on the network to avoid IP addresses conflict, and add a **Trustpoint**.

Navigate to **Configuration > Security > Web Auth > + Add** or select an parameter map:

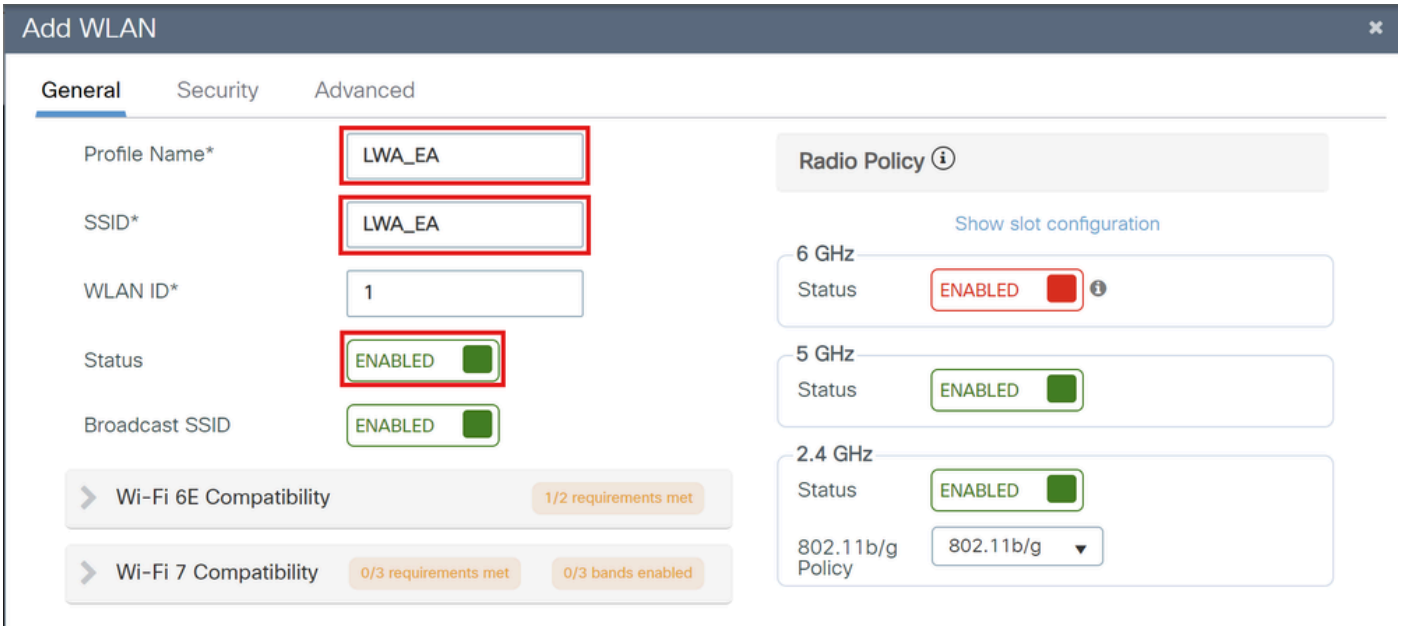


WebAuth Configuration

WLAN Configuration

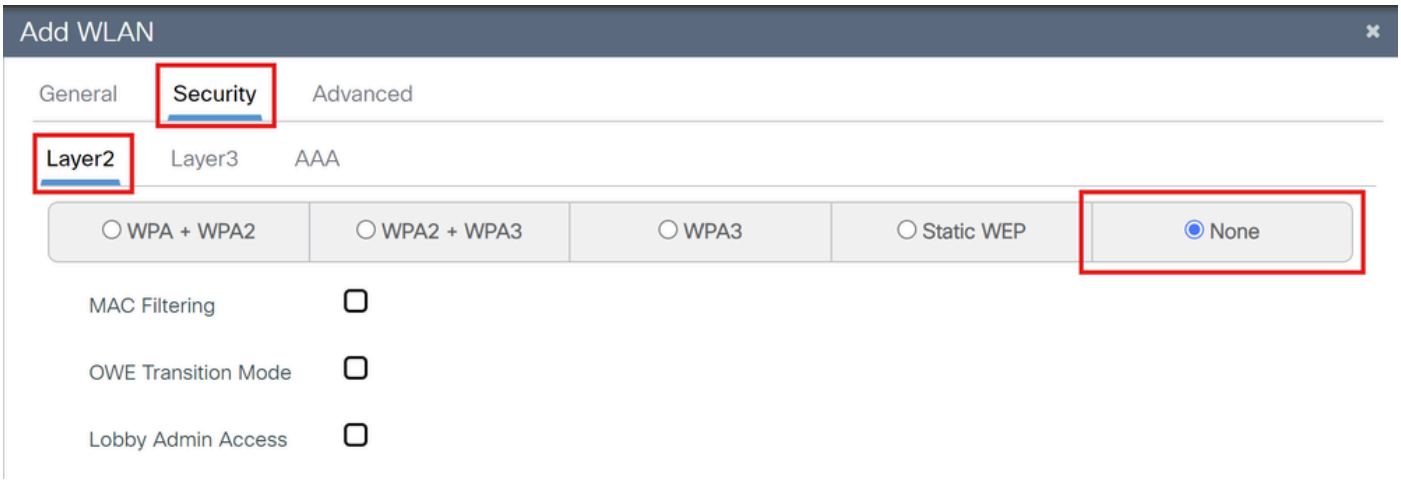
Step 1. Create the WLAN.

Navigate to **Configuration > Tags & Profiles > WLANs > + Add** and configure the network as needed.



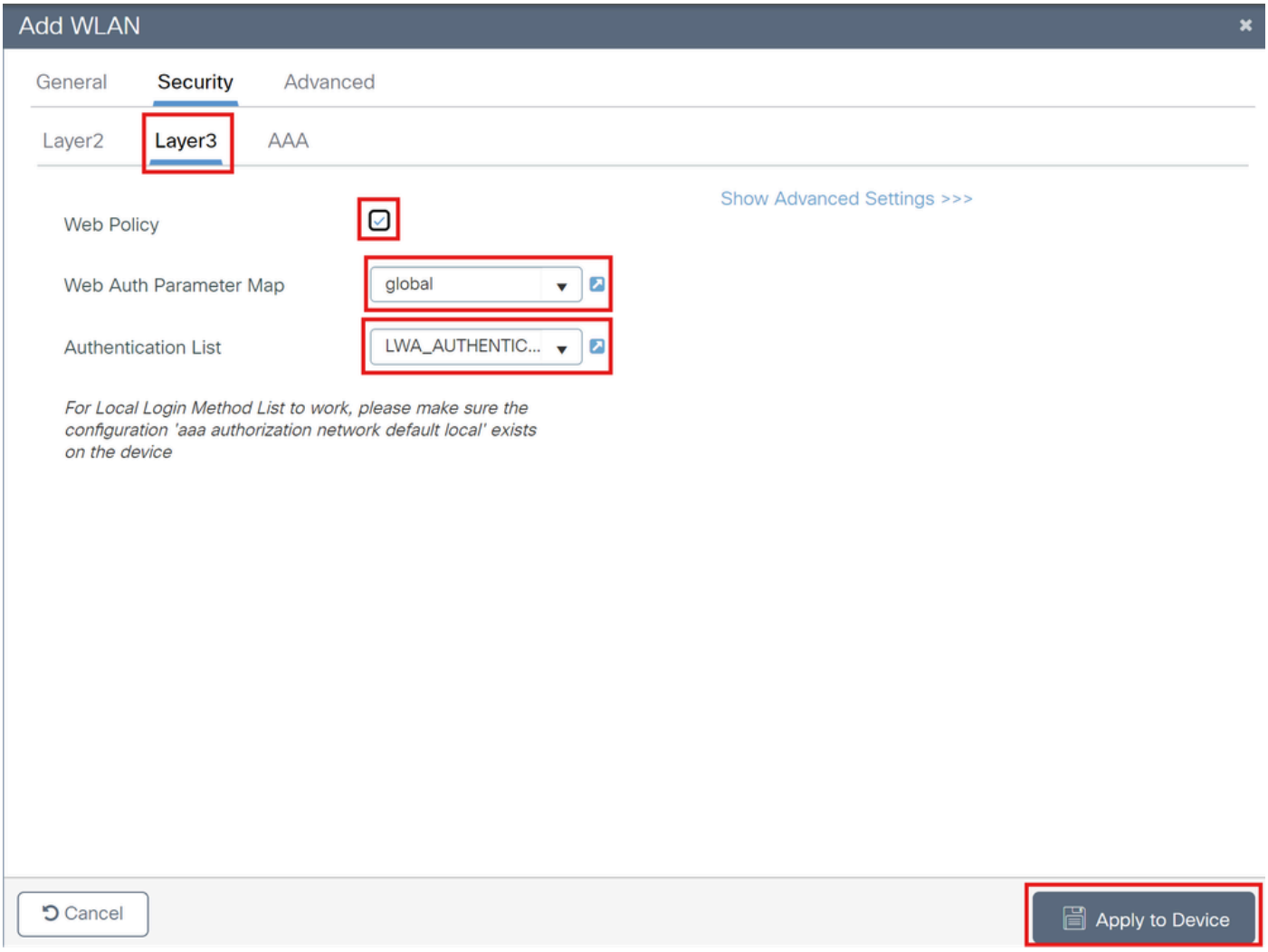
Create the WLAN

Step 2. Navigate to **Security > Layer2** and on **Layer 2 Security Mode** select **None**.



Create the WLAN Security

Step 3. Navigate to **Security > Layer3** and on **Web Policy** tick the box, on **Web Auth Parameter Map** select the parameter name, and on **Authentication List** select select the authentication list created previously.



Create the WLAN Authentication List

The WLAN is displayed on the WLAN list:



Created WLAN

Policy Profile Configuration

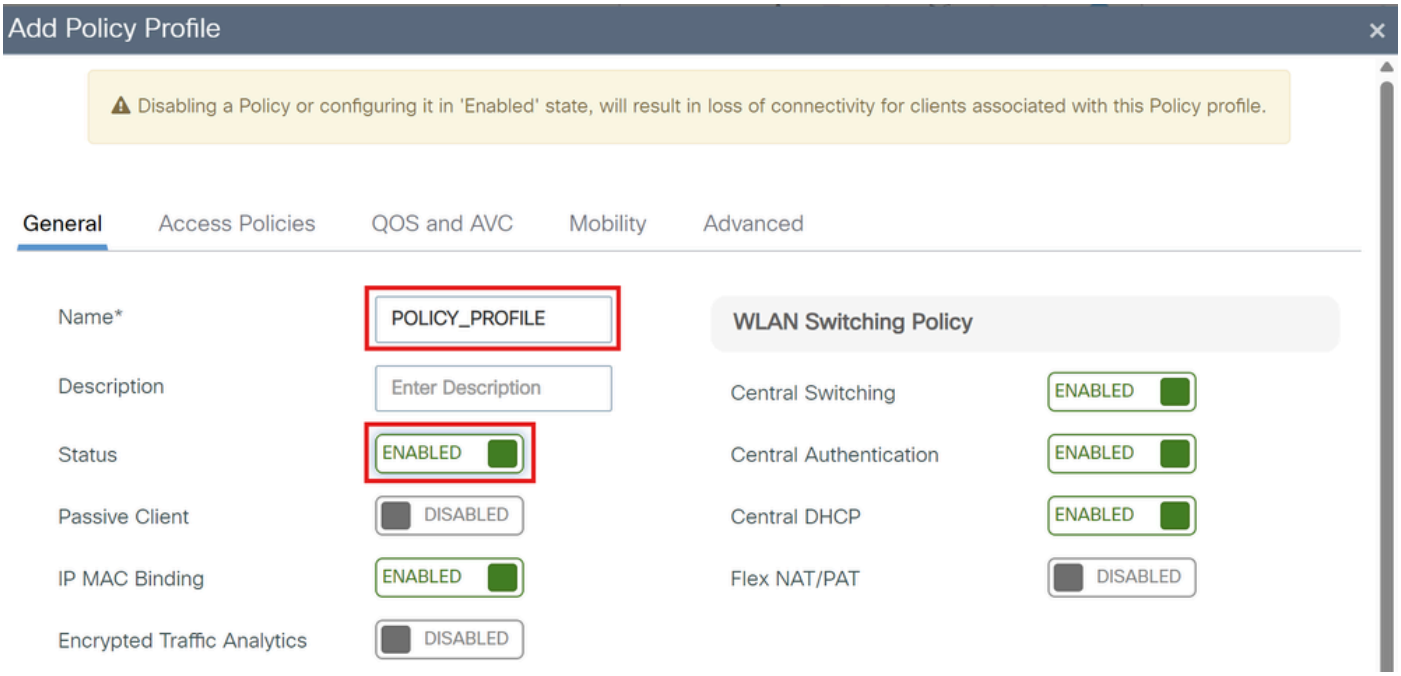
Inside a Policy Profile, you can select the VLAN that assigns the clients, among other settings.

You can either use your default policy profile or you can create a new one.

Step 1. Create a new **Policy Profile**.

Navigate to **Configuration > Tags & Profiles > Policy** and either configure your default policy profile or create a new one.

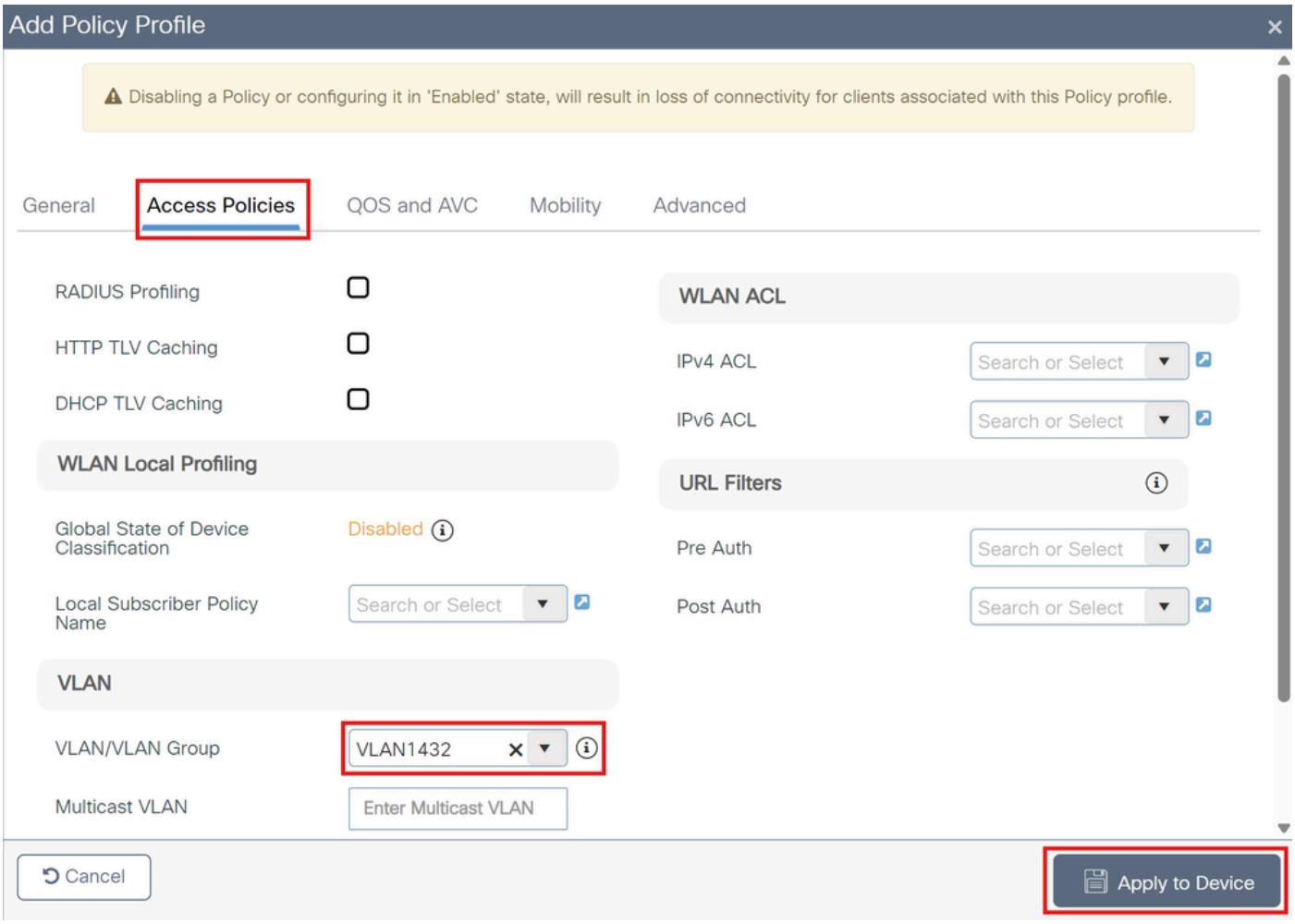
Ensure the profile is enabled.



Create a New Policy Profile

Step 2. Select the VLAN.

Navigate to the **Access Policies** tab and select the VLAN name from the drop-down or manually type the VLAN-ID.



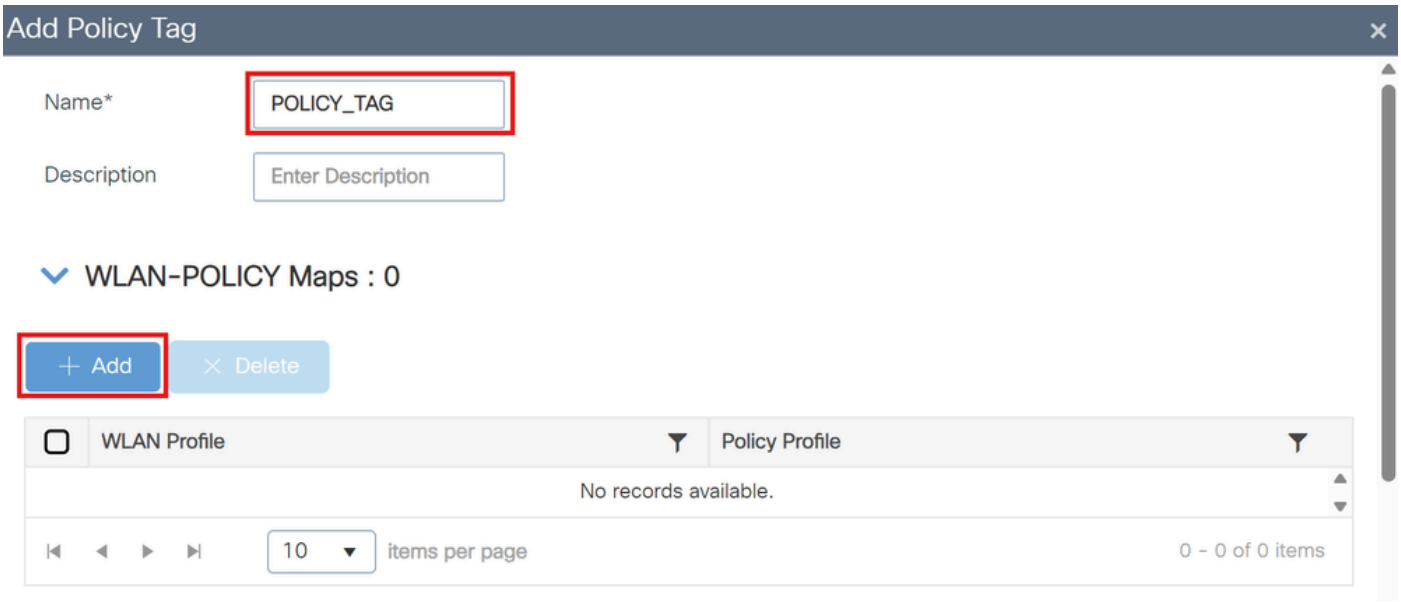
Select the VLAN

Policy Tag Configuration

Inside the Policy Tag is where you link your SSID with your Policy Profile. You can either create a new Policy Tag or use the default-policy tag.

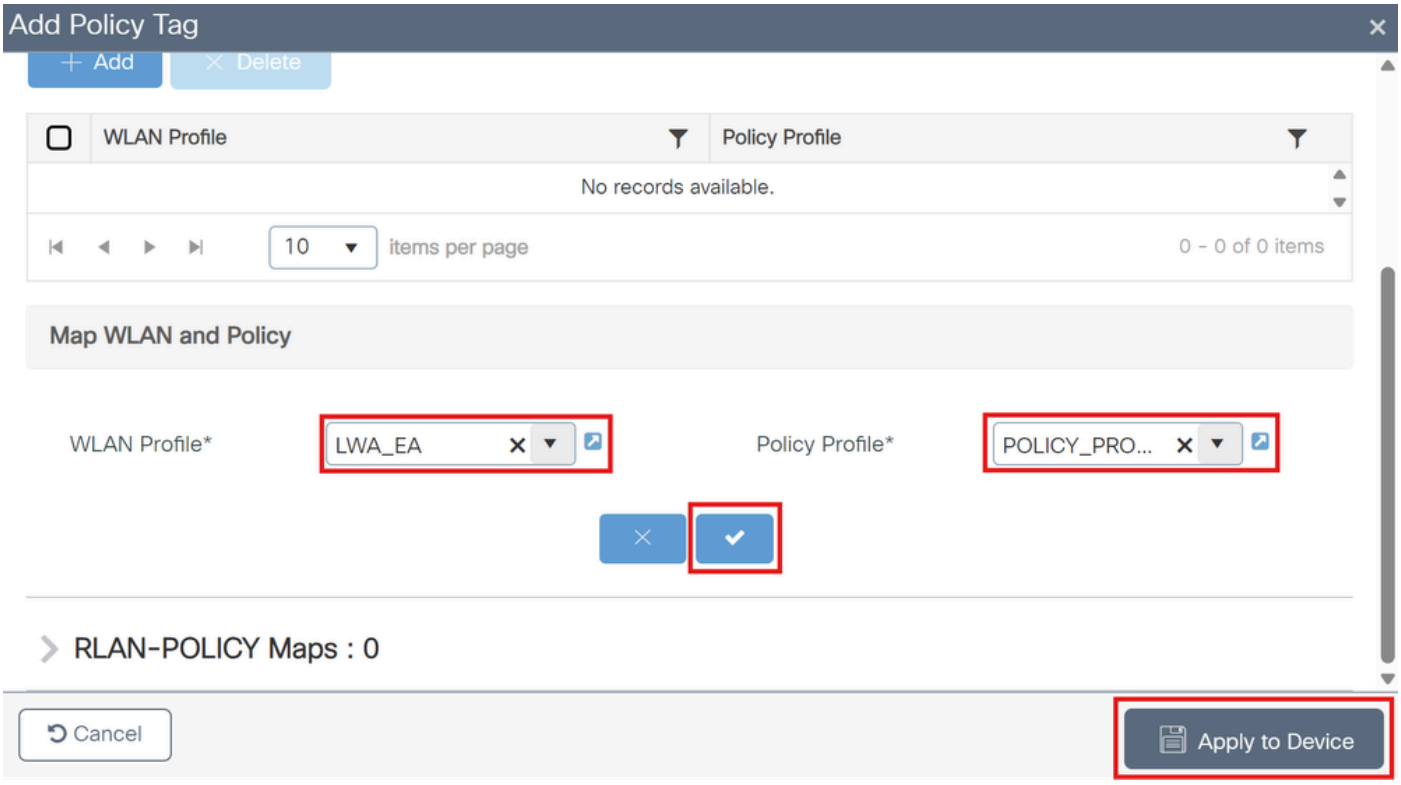
Navigate to **Configuration > Tags & Profiles > Tags > Policy** and add a new one if needed as shown in the image.

Select **+ Add:**



Policy Tag Configuration

Link your WLAN Profile to the desired Policy Profile:



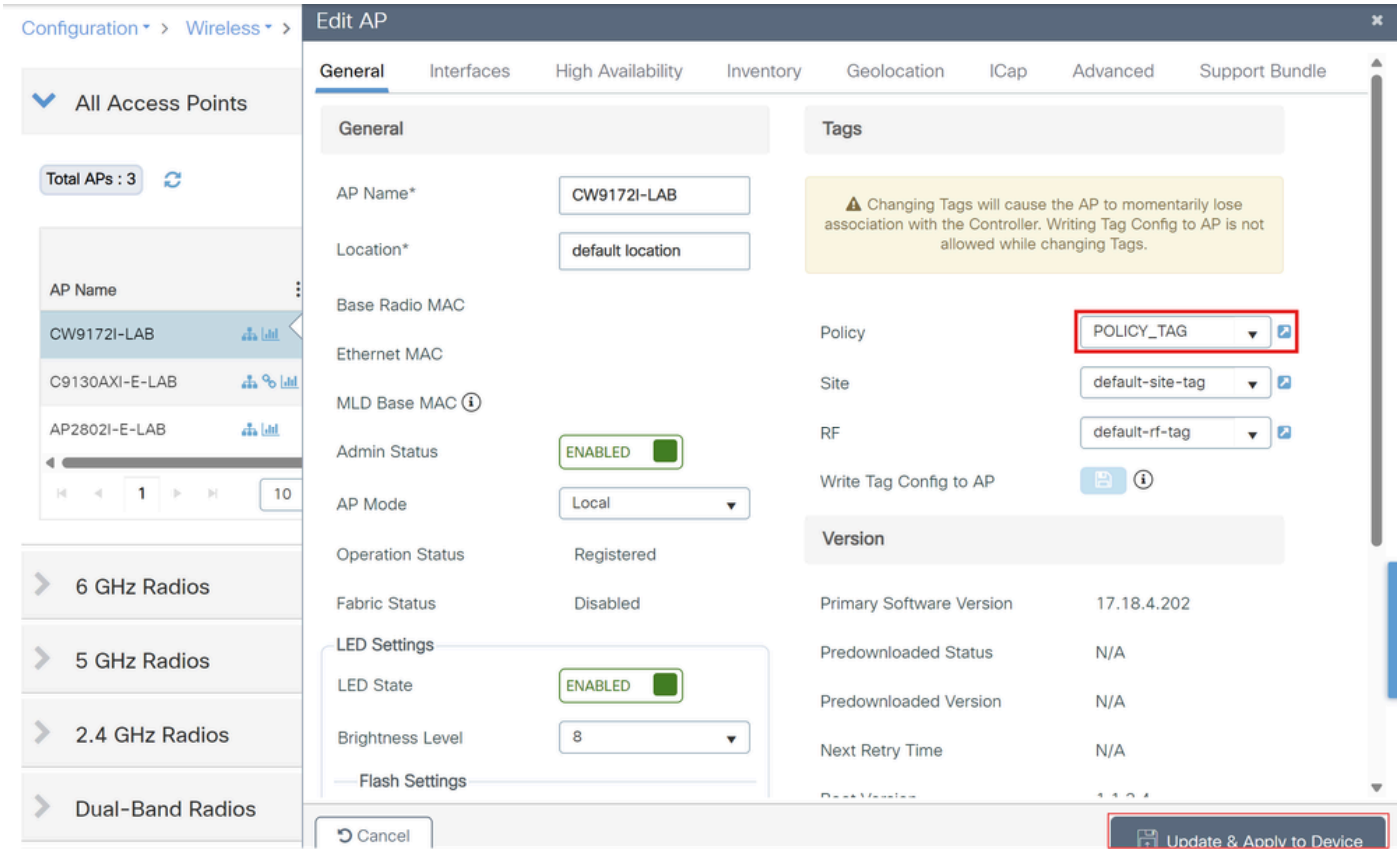
Policy Tag Configuration

Policy Tag Assignment

Assign the Policy Tag to the needed APs.

In order to assign the tag to one AP, navigate to **Configuration > Wireless > Access Points > AP Name >**

General Tags, make the needed assignment and then click **Update & Apply to Device.**

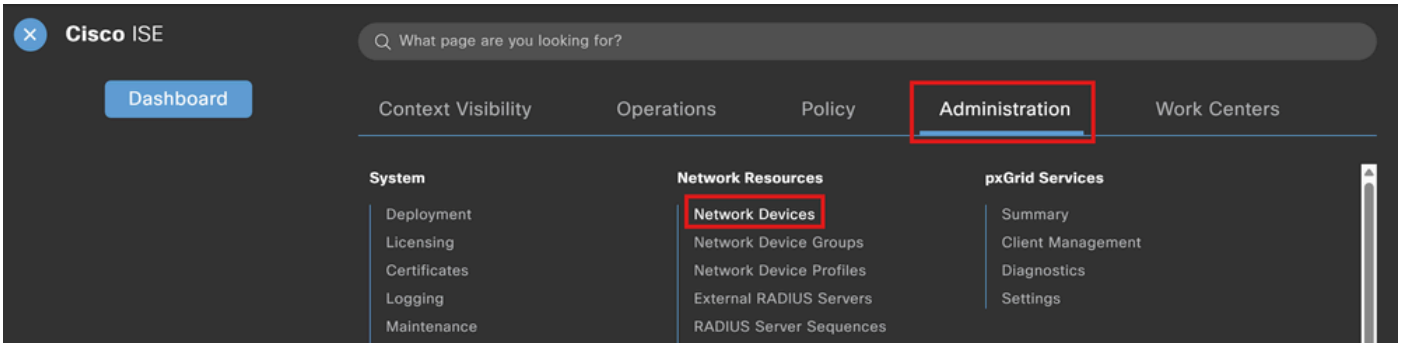


Policy Tag Assignment

ISE Configuration

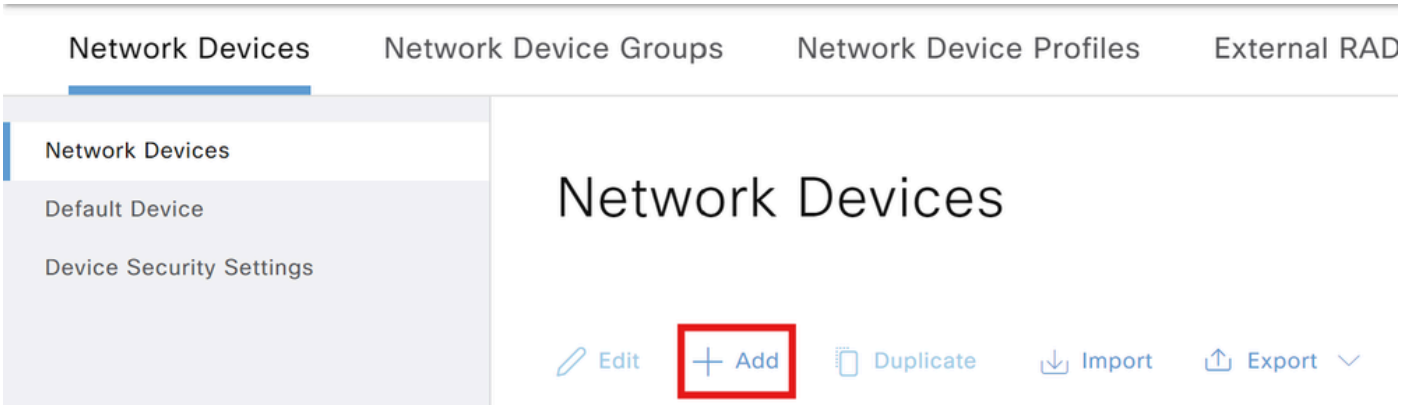
Add 9800 WLC to ISE

Step 1. Navigate to **Administration > Network Resources > Network Devices** as shown in the image.



Add 9800 WLC to ISE

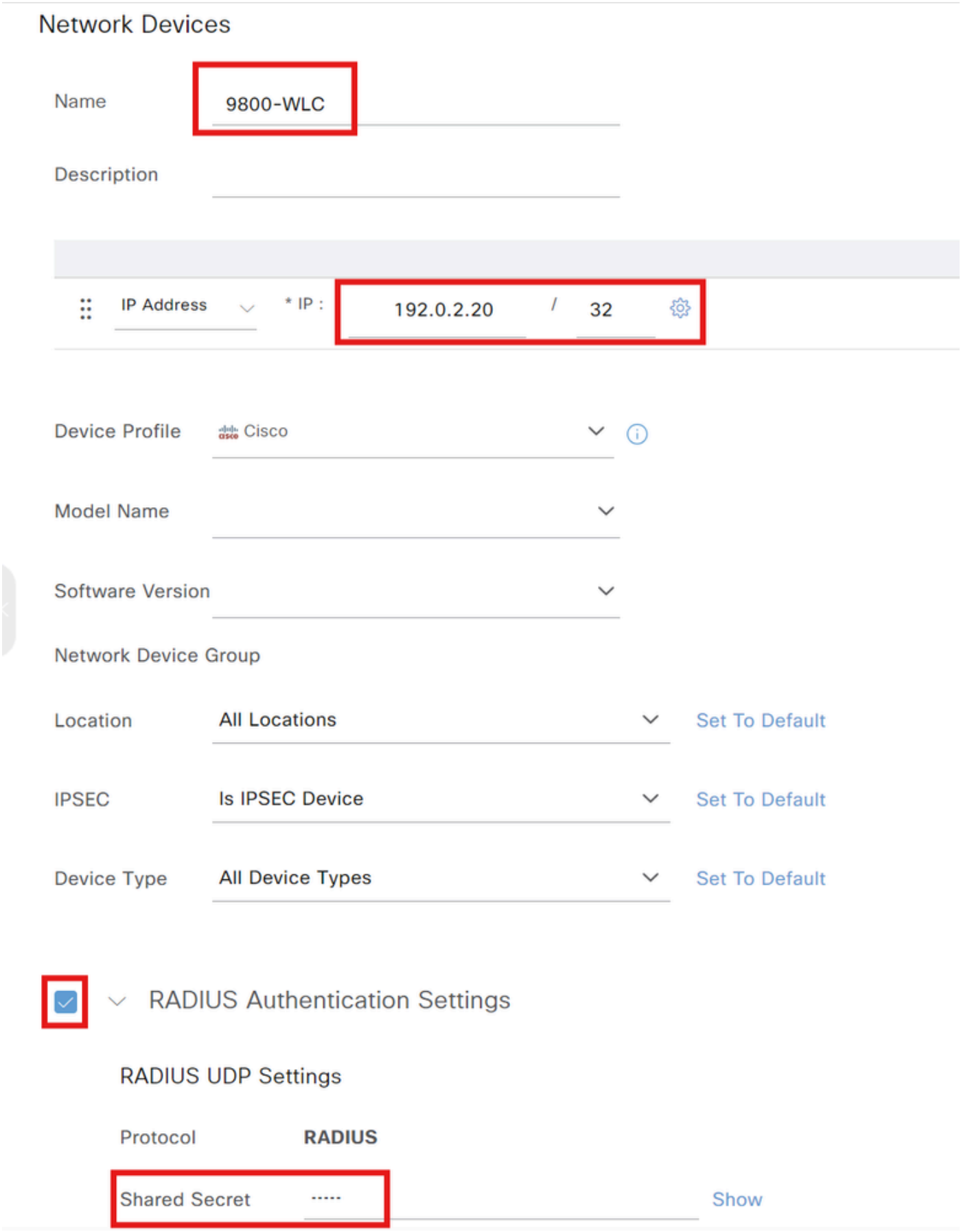
Step 2. Click +**Add**.



Add Network Devices

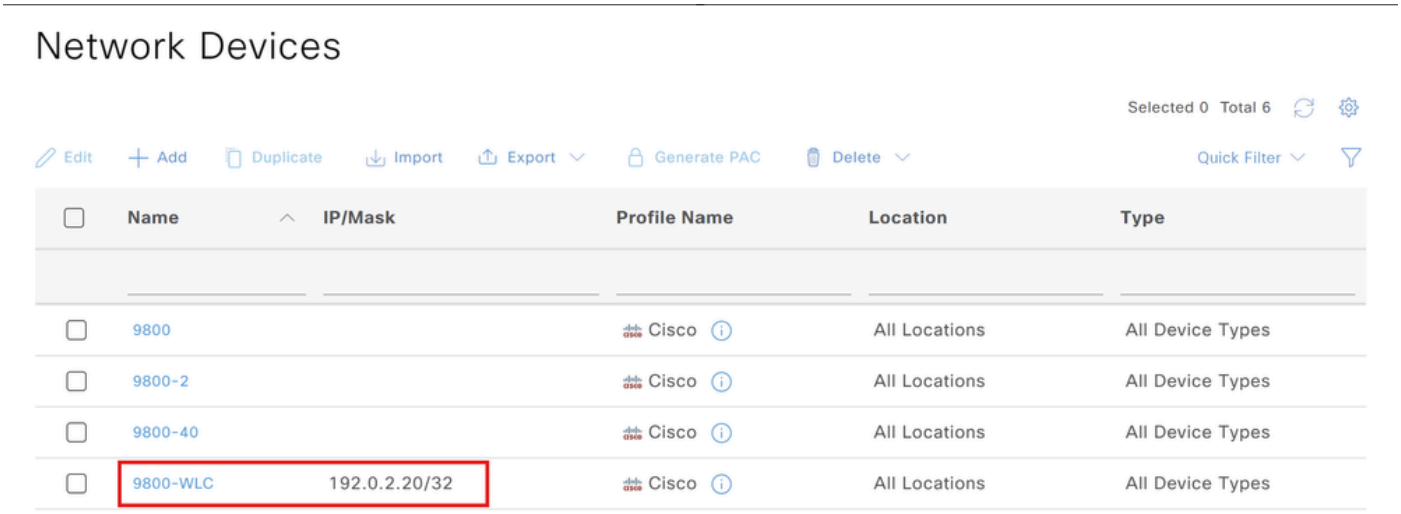
Optionally, it can be a specified Model name, software version, description, and assign Network Device groups based on device types, location or WLCs.

Step 3. Enter the 9800 WLC settings as shown in the image. Enter the same RADIUS key defined upon server creation on the WLC side. Then click **Submit**.



9800 WLC Settings

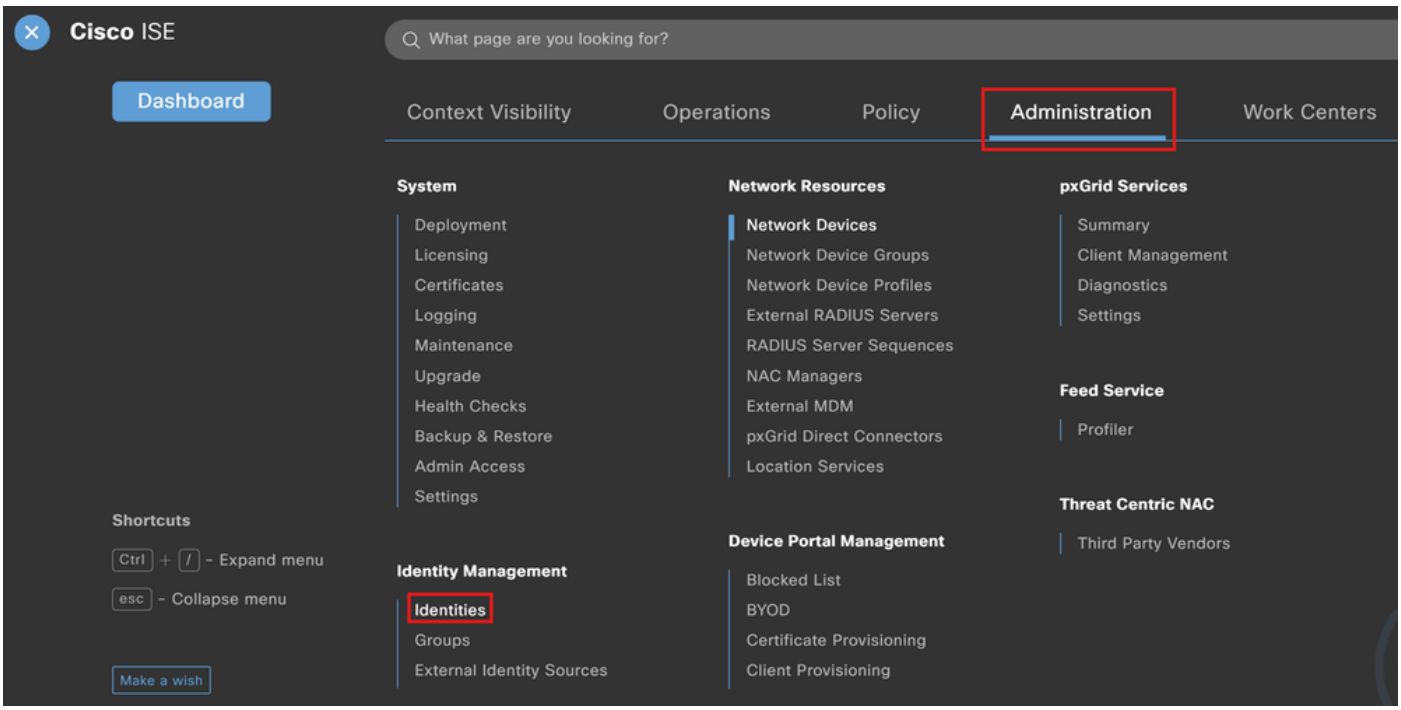
Step 4. Navigate to **Administration > Network Resources > Network Devices**, you can see the network devices list.



Network Devices List

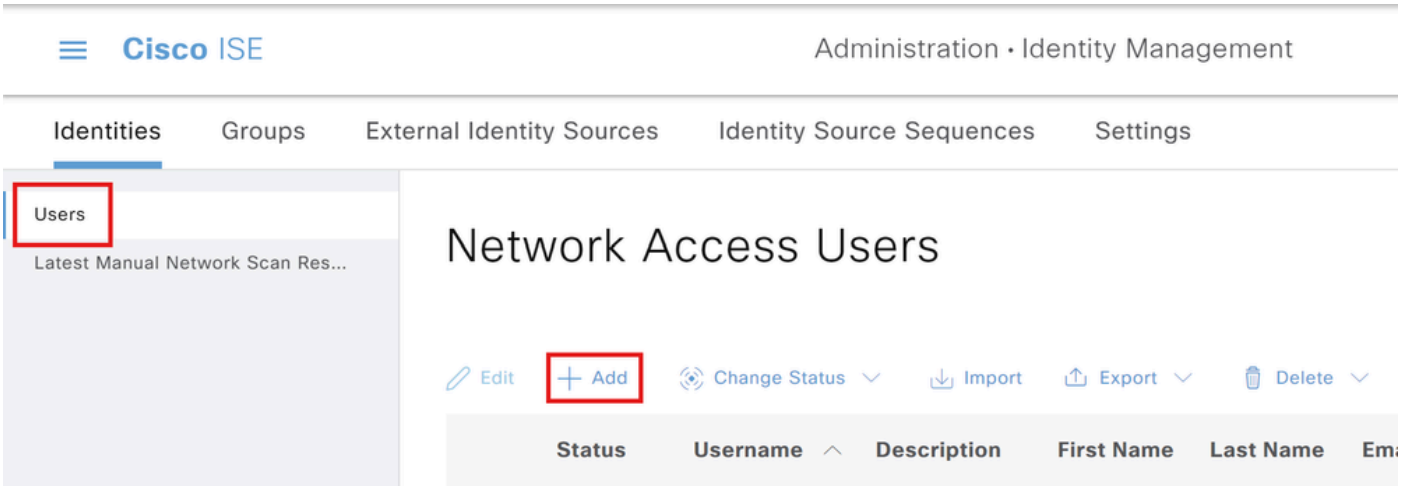
Create New User on ISE

Step 1. Navigate to **Administration > Identity Management > Identities:**



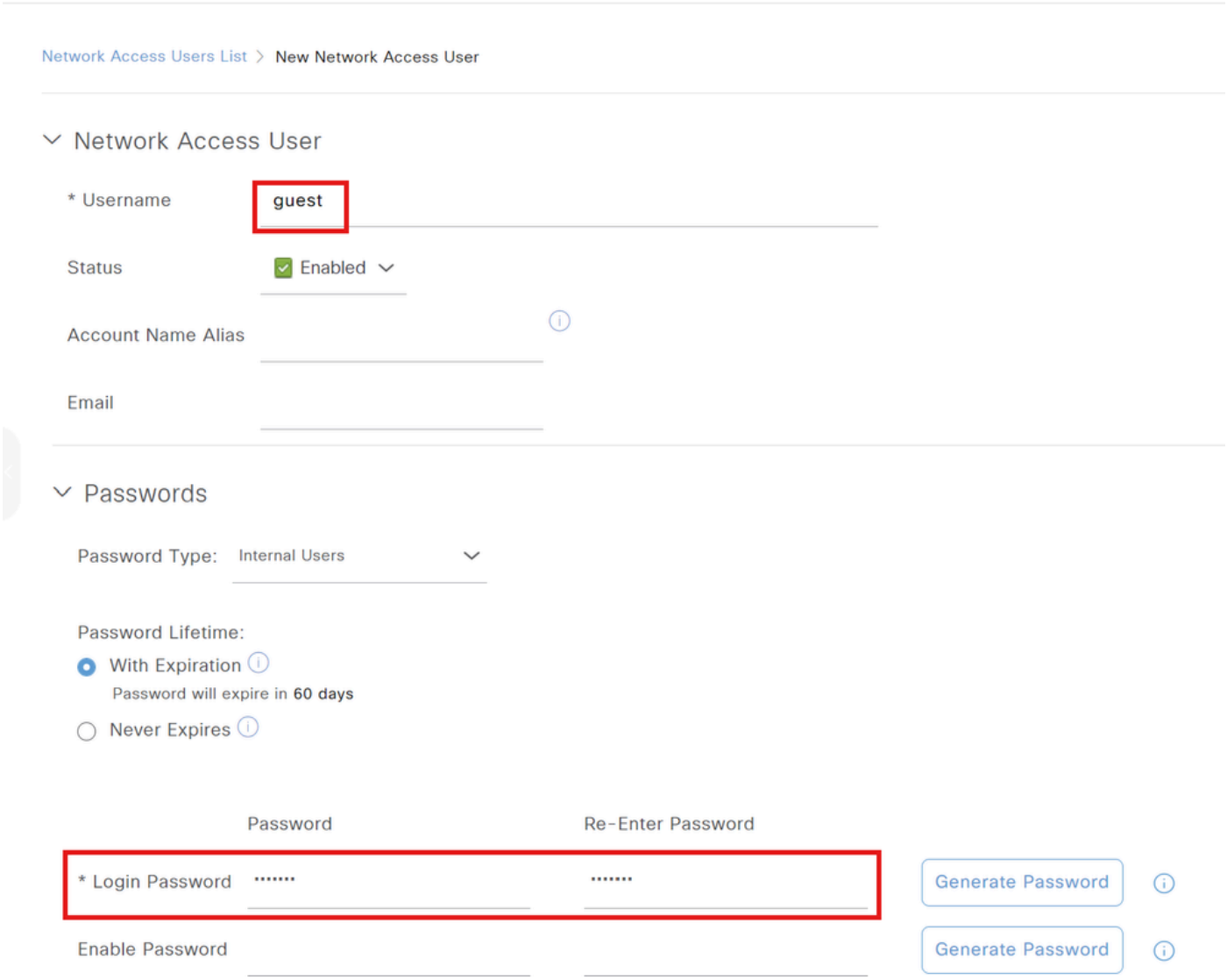
ISE Administration - Identities

Step 2. Navigate to **Users,** click **+Add**.



Add User

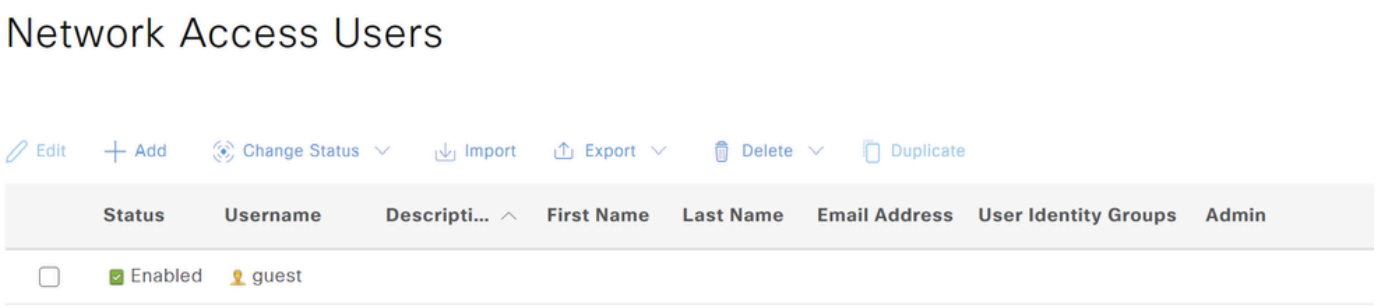
Step 3. Enter the username and password for the guest user, and click **Submit**.



Create New User on ISE

Step 4. Navigate to **Administration > Identity Management > Identities > Users**, you can see the users

list.



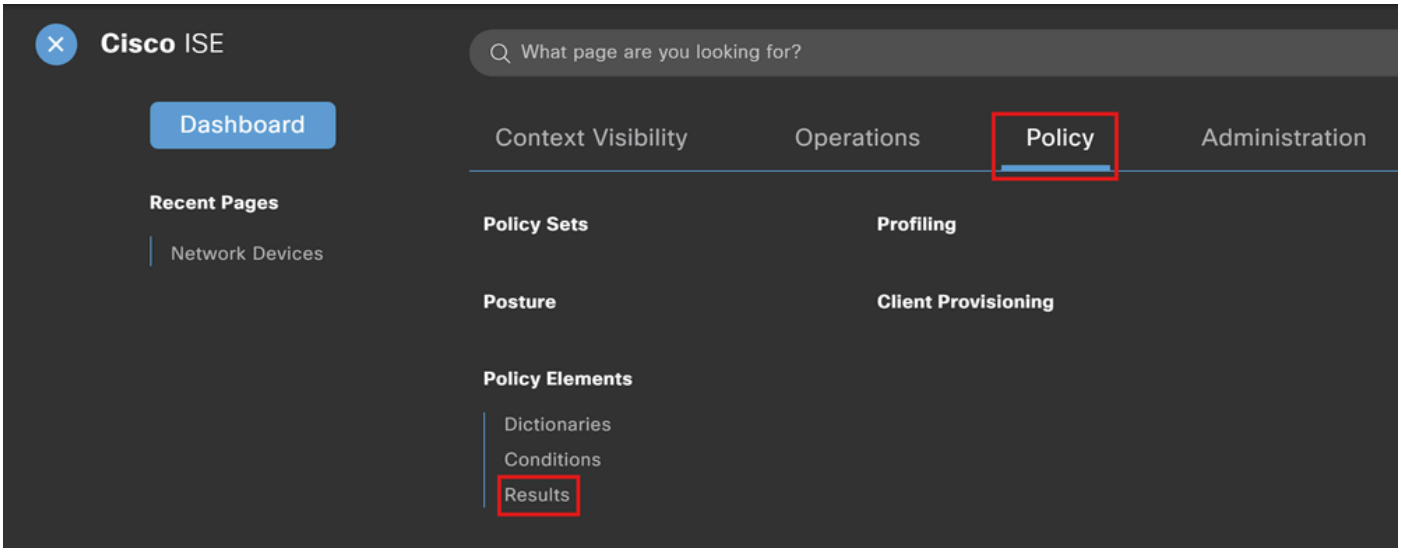
Network Access Users List

Create Authorization Profile

The policy profile is the result assigned to a client based on its parameters (as mac address, credentials, WLAN used and so on). It can assign specific settings like Virtual Local Area Network (VLAN), Access Control Lists (ACLs), Uniform Resource Locator (URL) redirects and so on.

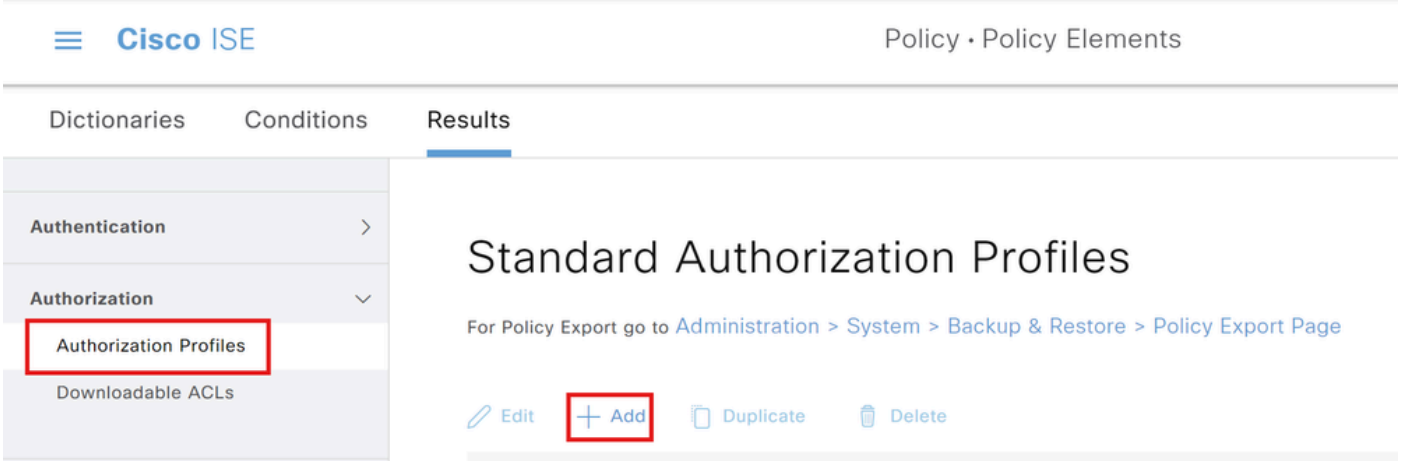
These steps show how to create the authorization profile needed to redirect the client to the authentication portal. Note that in recent versions of ISE, a Cisco_Webauth authorization result already exists. Here, you can edit it to modify the redirection ACL name in order to match what you configured on the WLC.

Step 1. Navigate to **Policy > Policy Elements > Results.**



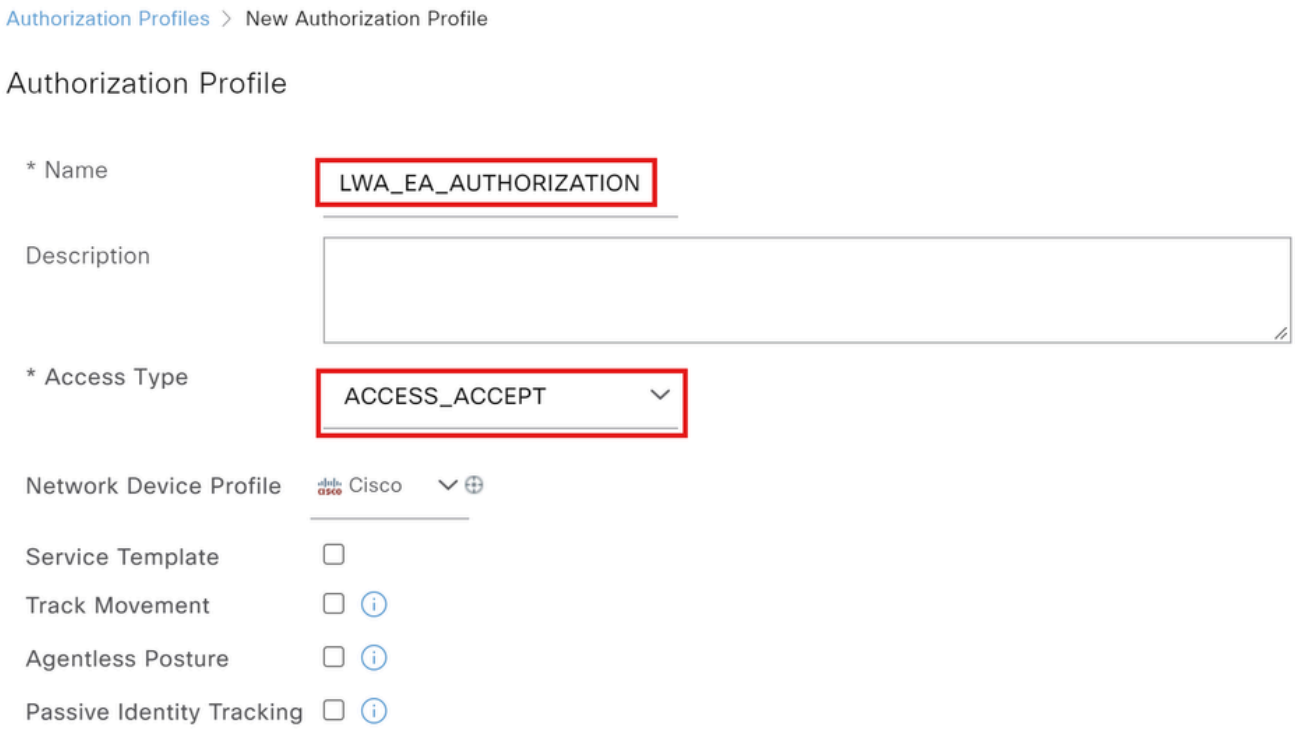
ISE Policy - Results

Step 2. Navigate to **Authorization > Authorization Profiles.** Click **+Add** in order to create authorization profile.



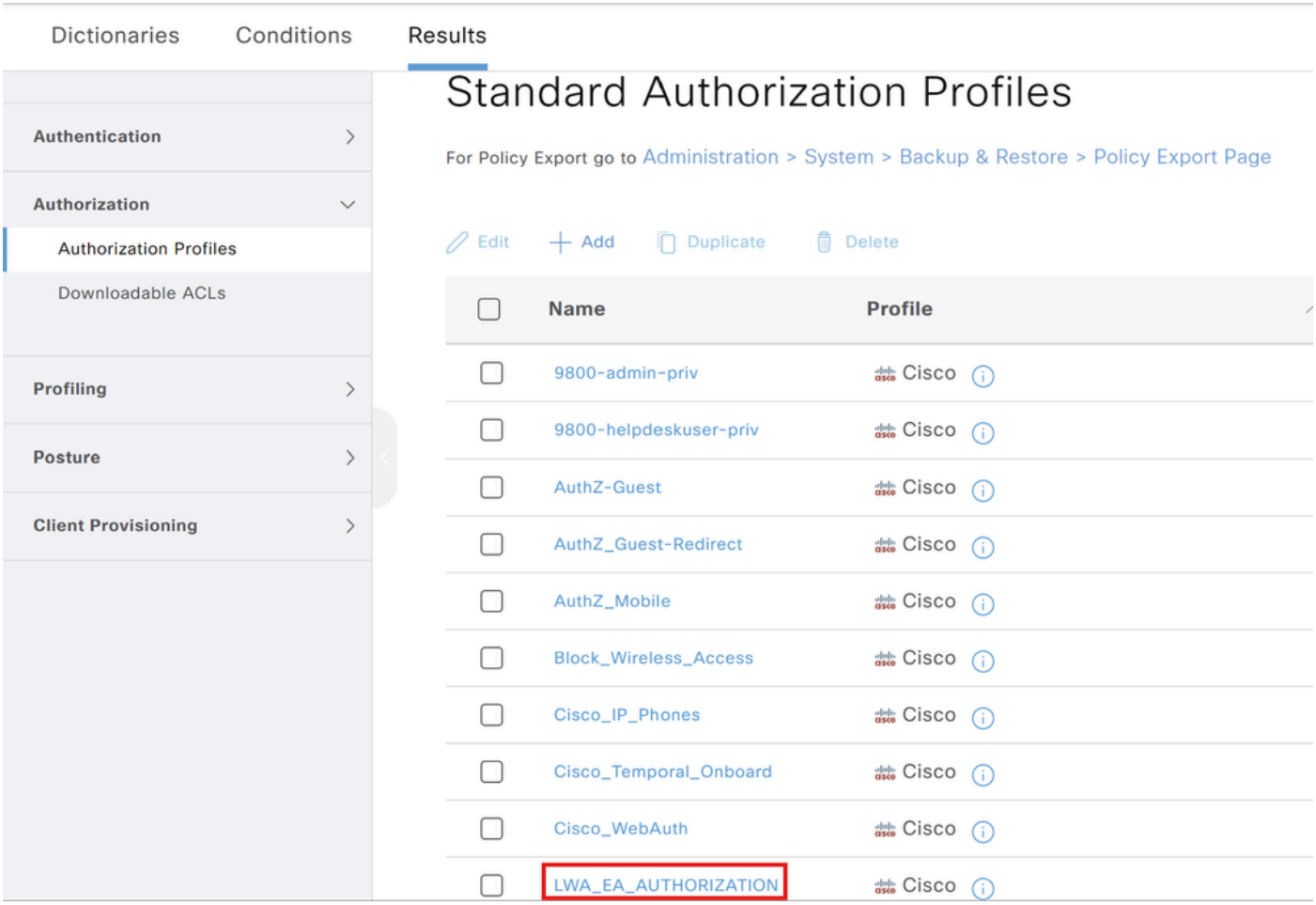
Add Authorization Profile

Step 3. Create the authorization profile **LWA_EA_AUTHORIZATION**. The Attributes Details must be Access Type=ACCESS_ACCEPT. Click **Submit**.



Create Authorization Profile

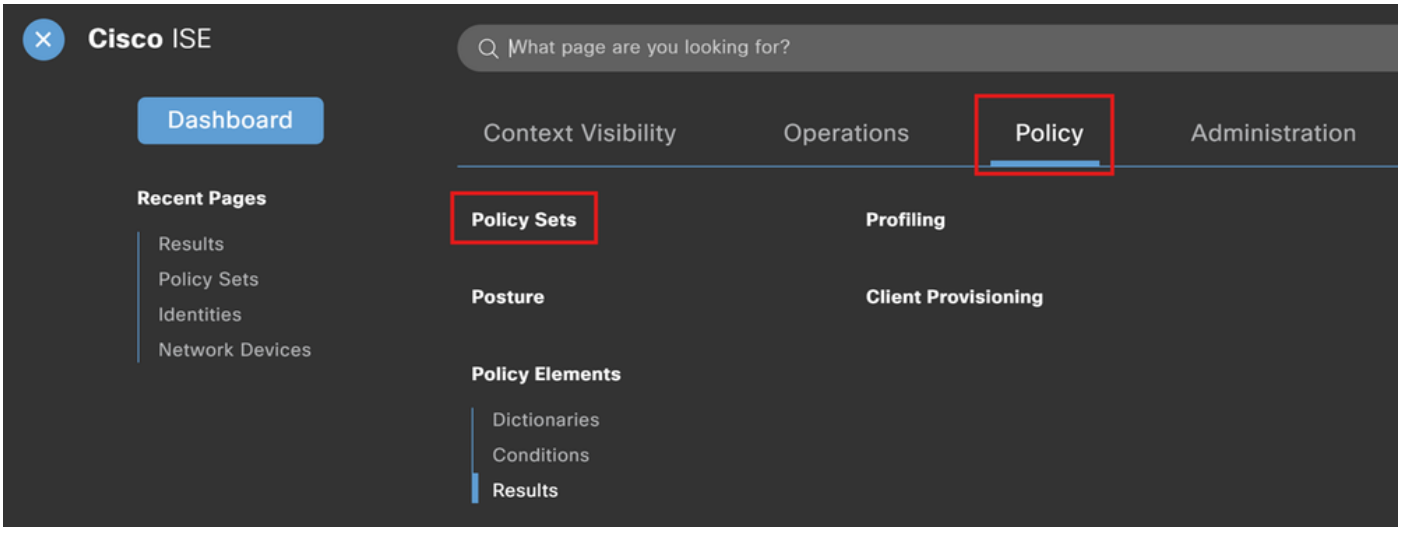
Step 4. Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles,** you can see the authorization profiles.



Authorization Profiles List

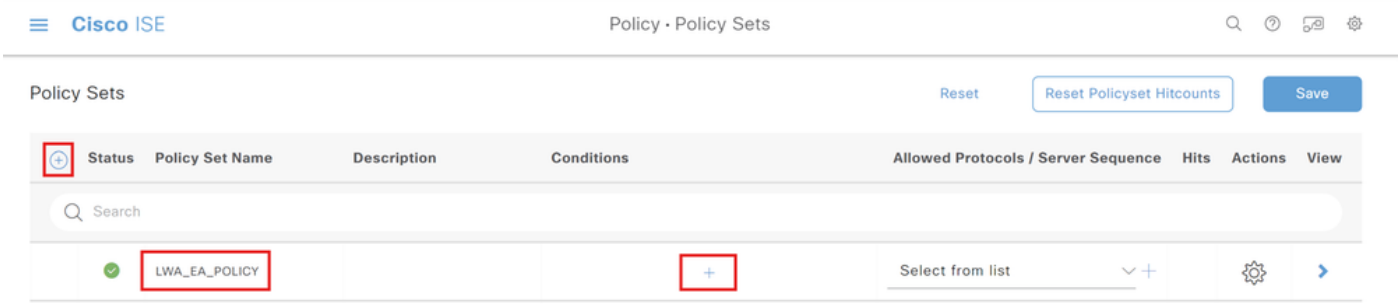
Configure Authentication Rule

Step 1. Navigate to **Policy > Policy Sets**.



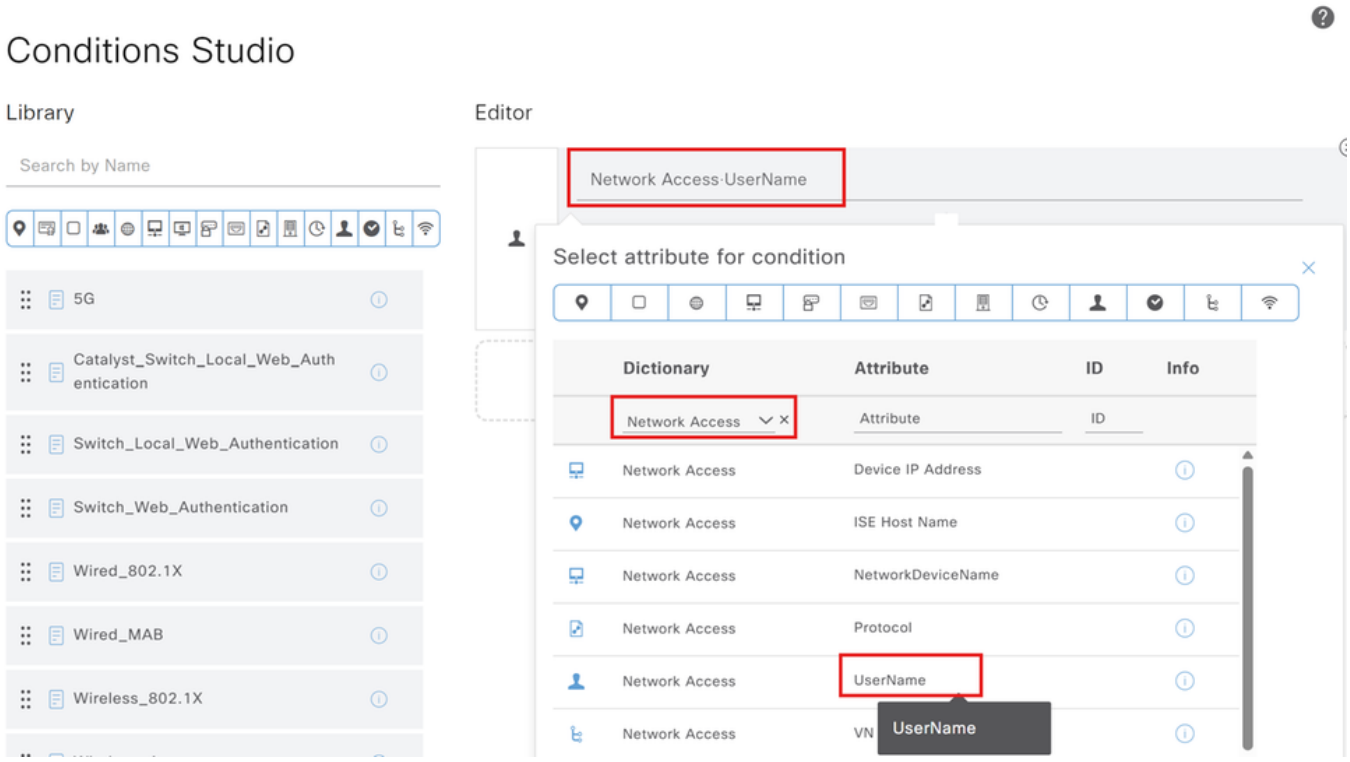
ISE Policy - Policy Sets

Step 2. Select the + sign, type the name of the policy set **LWA_EA_POLICY**. Click on the column **Conditions.**



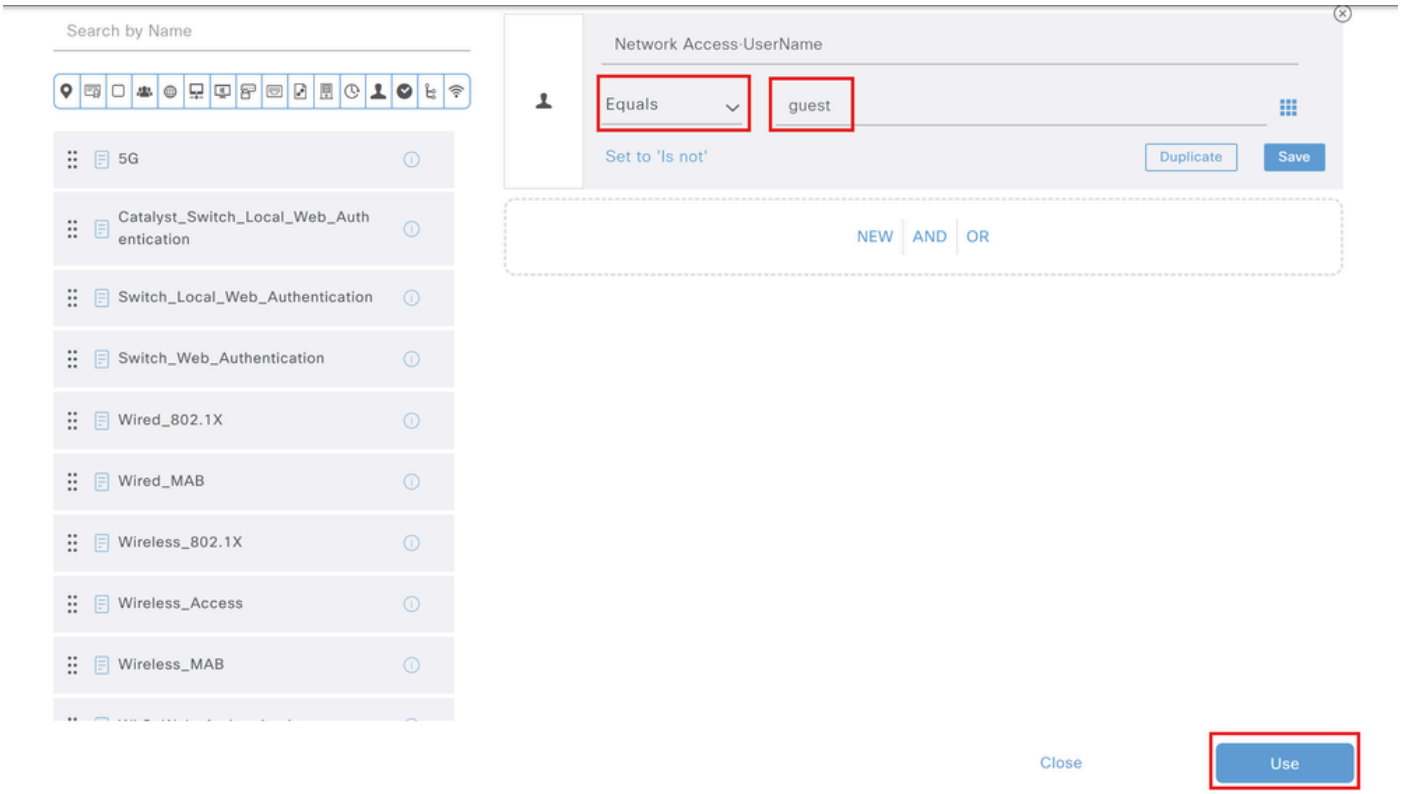
Configure Authentication Rule

Step 3. On **Dictionary** select **Network Access**. On **Attribute** select **Username**.



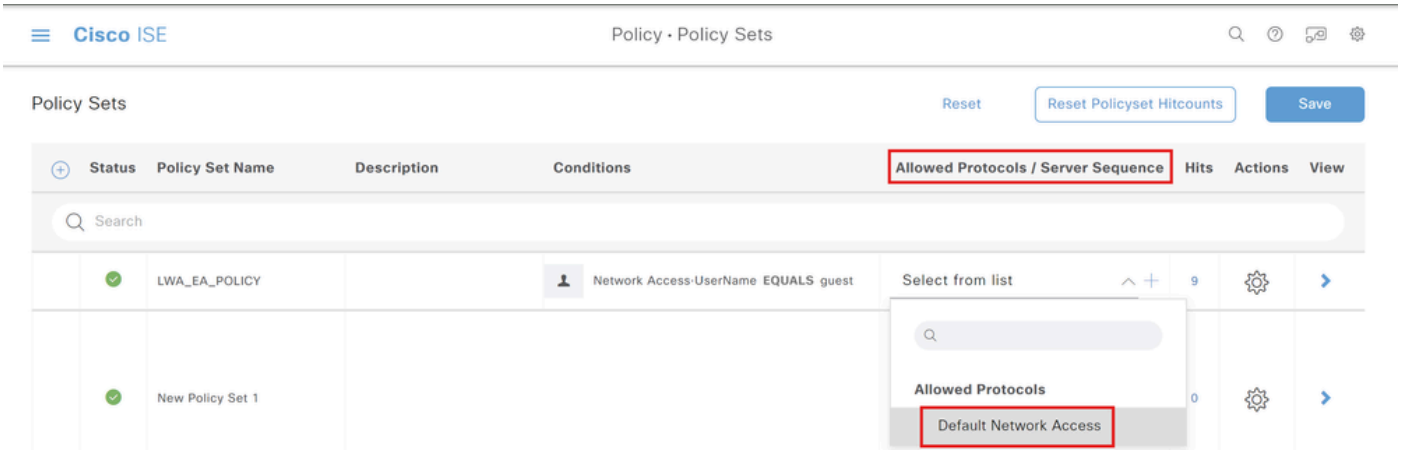
Dicionary Network Access

Step 4. Set **Equals** and type **guest** on the text box (the username defined on **Administration > Identity Management > Identities > Users**). Click **Save** in order to save the changes.



Username Guest

Step 5. Navigate to **Policy > Policy Sets**. On the policy set you created, on column **Allowed Protocols/Server Sequence** select **Default Network Access**.



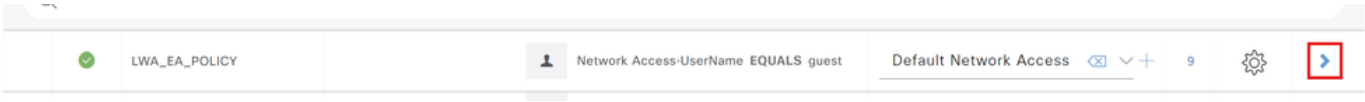
Policy Sets

Step 6. Click **Save** in order to save the changes.

Configure Authorization Rules

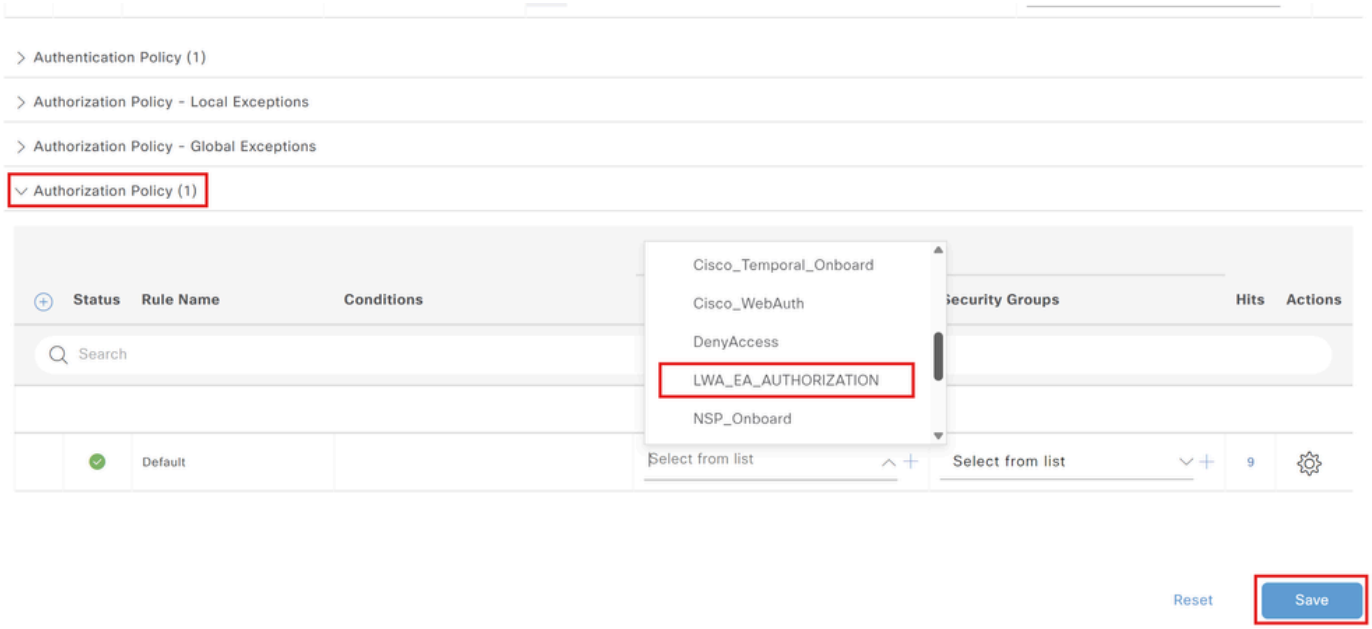
The authorization rule is the one in charge to determine which permissions (which authorization profile) result is applied to the client.

Step 1. Navigate to **Policy > Policy Sets**. Click on the arrow icon on the policy set you created.



Policy Set Arrow

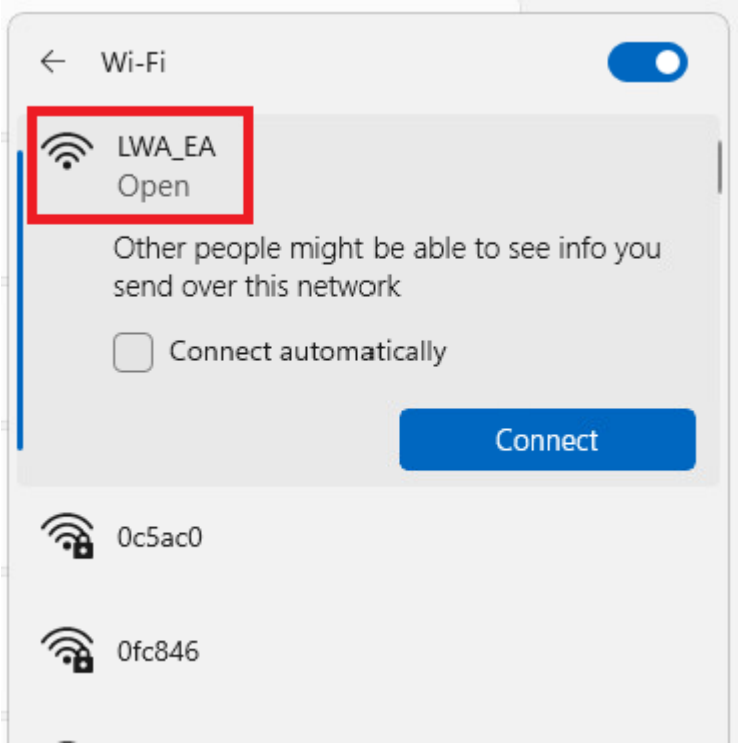
Step 2. On the same Policy set page, expand **Authorization Policy** as shown in the image. On **Profiles** column delete **DenyAccess** and add **LWA_EA_AUTHORIZATION**. Click **Save** in order to save the changes.



Authorization Policy

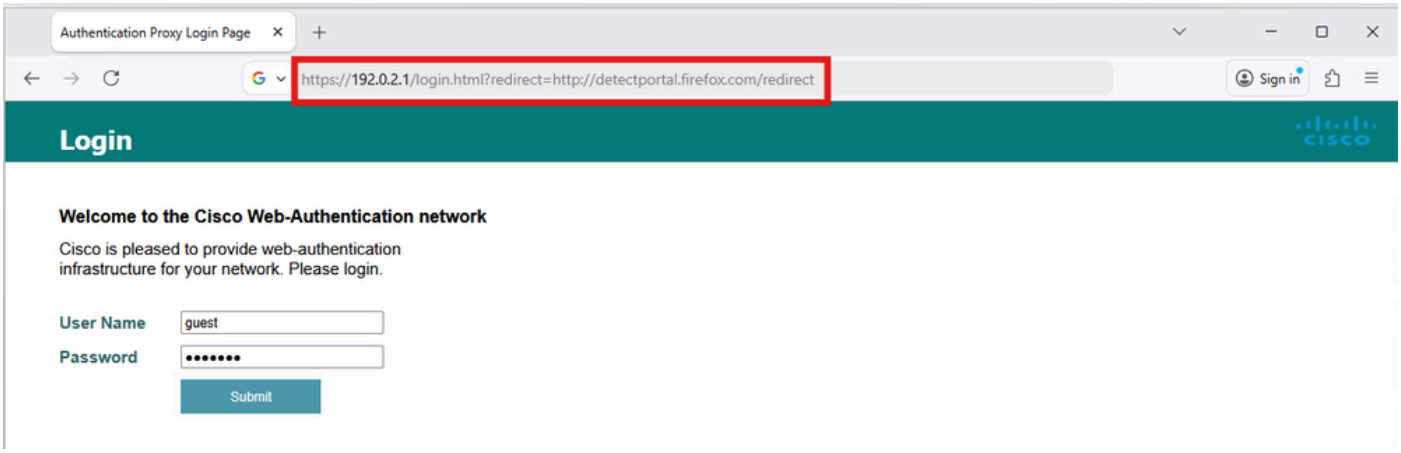
Connect Guest Client

Step 1. On your computer/phone navigate to the Wi-Fi networks, find the SSID **LWA_EA** and select **Connect**.



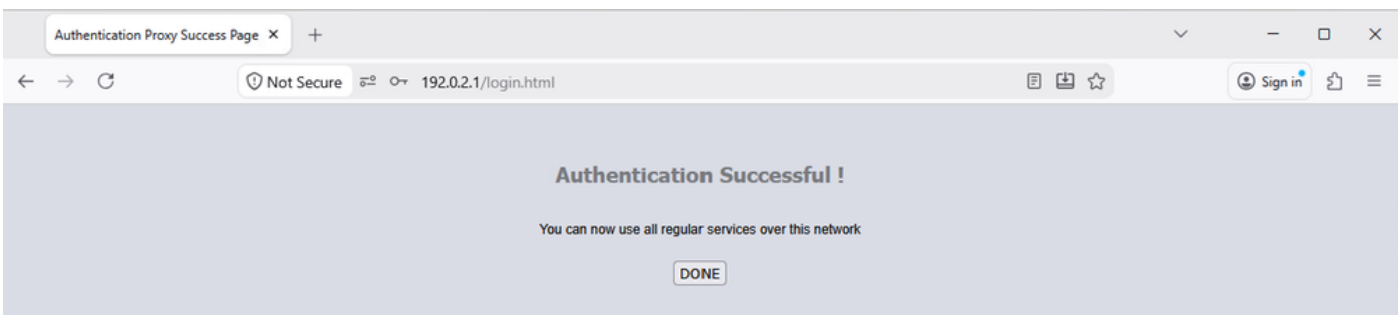
Connect Guest Client

Step 2. A browser window pops up, with the log in page. The redirect URL is in the URL box, and you have to type the **Username** and **Password** to gain access to the network. Then select **Submit**.



Login Page with Redirect URL

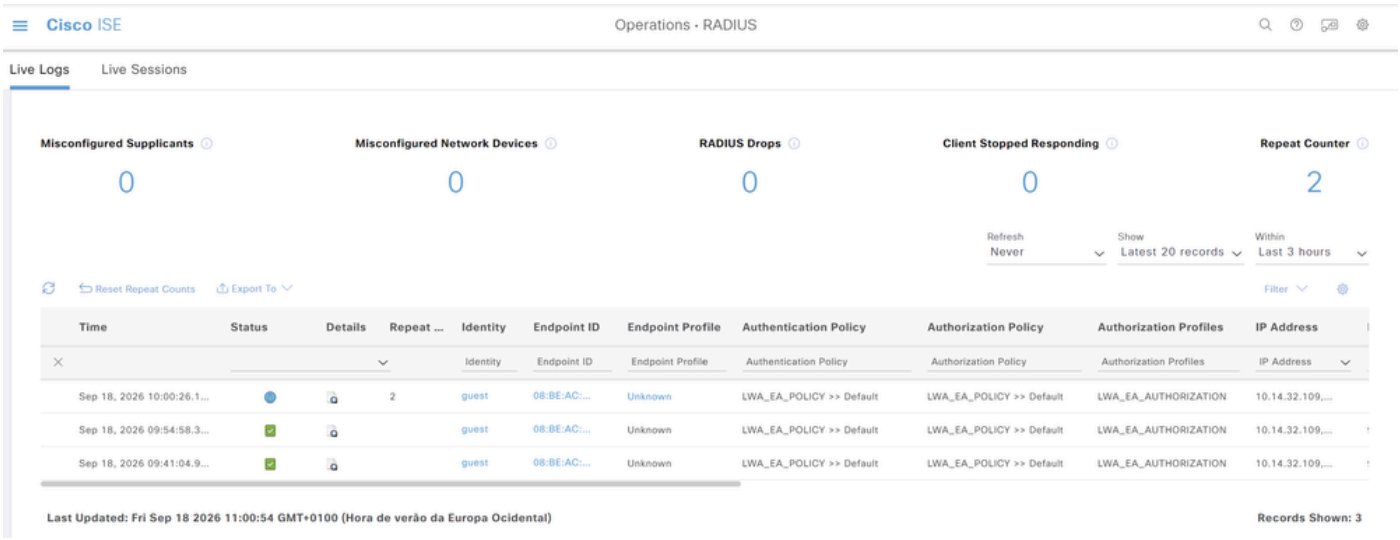
If the credentials are correct, an authentication successful page appears:



Authentication Successful Login Page

Note: The URL presented was provided by the WLC. It contains the WLC Virtual IP and the redirect for the Windows connect test URL.

Step 3. Navigate to **Operations > RADIUS > Live Logs**. You can see the client device authenticated, along with its authentication and authorization policies.



Radius Live Logs

Verify

Use this section in order to confirm that your configuration works properly.

Show WLAN Summary

<#root>

9800WLC#show wlan summary

```
Number of WLANs: 1
ID Profile Name SSID Status 2.4GHz/5GHz Security
-----------------------------------------------
```

1 LWA_EA LWA_EA UP [open],[Web Auth]

9800WLC#

show wlan name LWA_EA

```
WLAN Profile Name : LWA_EA
=================================================
Identifier : 1
Description :
Network Name (SSID) : LWA_EA
Status : Enabled
Broadcast SSID : Enabled
Advertise-Apname : Disabled
Universal AP Admin : Disabled
(...)
Accounting list name :
802.1x authentication list name : Disabled
802.1x authorization list name : Disabled
Security

Web Based Authentication : Enabled


OWE Transition Mode : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled

Webauth Authentication List Name : LWA_AUTHENTICATION



Webauth Authorization List Name : Disabled



Webauth Parameter Map : global


(...)
Security-2.4GHz/5GHz

802.11 Authentication : Open System


Static WEP Keys : Disabled

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled


OSEN : Disabled
PMF Support : Disabled
(...)
Band Select : Disabled
Load Balancing : Disabled
(...)
```

Show Parameter Map Configuration

```
9800WLC#show running-config | section parameter-map type webauth global

parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
trustpoint TP-self-signed-123456
```

Show AAA Information

```
<#root>

9800WLC#show aaa method-lists authentication

authen queue=AAA_ML_AUTHEN_LOGIN

name=LWA_AUTHENTICATION valid=TRUE id=BD000005 :state=ALIVE : SERVER_GROUP RADIUSGROUP


authen queue=AAA_ML_AUTHEN_ENABLE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
(...)

9800WLC#show aaa method-lists authorization

author queue=AAA_ML_AUTHOR_SHELL
author queue=AAA_ML_AUTHOR_NET

name=LWA_AUTHORIZATION valid=TRUE id=90000006 :state=ALIVE : SERVER_GROUP RADIUSGROUP


author queue=AAA_ML_AUTHOR_CONN
author queue=AAA_ML_AUTHOR_IPMOBILE
author queue=AAA_ML_AUTHOR_RM
(...)

9800WLC#show aaa servers


RADIUS: id 2, priority 1, host 192.0.2.30, auth-port 1812, acct-port 1813, hostname RADIUS


State: current UP, duration 8421s, previous duration 0s
Dead: total time 0s, count 0
Platform State from SMD: current UP, duration 8421s, previous duration 0s
SMD Platform Dead: total time 0s, count 0
Platform State from WNCD (0) : current UP
(...)
```

Troubleshoot

Common Issues

These are several guides on how to troubleshoot Web Authentication issues, such as:

- Users cannot authenticate.
- Certificate problems.
- Redirection URL does not work.
- Guest users cannot connect to the guest WLAN.
- Users do not obtain an IP address.
- Redirection to the Web Authentication Log in Page fails.
- After successful Authentication, guest users fail to get access to the Internet.

These guides describe troubleshoot steps in detail:

- Troubleshoot Common Issues for Web Authentication
- Other Situations to Troubleshoot

Conditional Debug and Radio Active Trace and Embedded Packet Capture

You can enable conditional debug and capture Radio Active (RA) trace, which provides debug level traces for all processes that interact with the specified condition (client mac address in this case). In order to enable conditional debug, use the steps in the guide, Conditional Debug and RadioActive trace.

You can also collect Embedded Packet capture (EPC). EPC is a packet capture facility that allows a view into packets destined to, sourced from, and passes through the Catalyst 9800 WLCs, namely DHCP, DNS, HTTP GET packets in LWA. These captures can be exported for offline analysis with Wireshark. For detailed steps on how to do this, refer to Embedded Packet Capture.

Example of a Successful Attempt

This is the output from the RA_traces for a successful attempt to identify each of the phases upon the association/authentication process, while in connection to a guest SSID with RADIUS server.

802.11 association/authentication:

```
[client-orch-sm] [17062]: (note): MAC: 08be.ac3f Association received. BSSID cc70.edcf.552f, WLAN LWA_EA, Slot 1 AP 2ce3.8eb4, CW9172I-LAB
[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Received Dot11 association request. Processing started,SSID: LWA_EA, Policy profile: POLICY_PROFILE, AP Name: CW9172I-LAB, Ap Mac Address: 2ce3.8eb4BSSID MAC0000.0000.0000wlan ID: 1RSSI: -49, SNR: 46
[client-orch-state] [17062]: (note): MAC: 08be.ac3f Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
[dot11-validate] [17062]: (info): MAC: 08be.ac3f Dot11 ie validate ext/supp rates. Validation Passed for Supported rates radio_type 2
[dot11-validate] [17062]: (info): MAC: 08be.ac3f WiFi direct: Dot11 validate P2P IE. P2P IE not present.
```

[dot11] [17062]: (debug): MAC: 08be.ac3f dot11 send association response. Framing association response with resp_status_code: 0
[dot11] [17062]: (debug): MAC: 08be.ac3f Dot11 Capability info byte1 1, byte2: 11
[dot11-frame] [17062]: (info): MAC: 08be.ac3f WiFi direct: skip build Assoc Resp with P2P IE: Wifi direct policy disabled
[dot11] [17062]: (info): MAC: 08be.ac3f dot11 send association response. Sending assoc response of length: 130 with resp_status_code: 0, DOT11_STATUS: DOT11_STATUS_SUCCESS
[dot11] [17062]: (note): MAC: 08be.ac3f Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False Fast roam = False
[dot11] [17062]: (info): MAC: 08be.ac3f DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED
[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Station Dot11 association is successful.

IP Learn process:

[client-orch-state] [17062]: (note): MAC: 08be.ac3f Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
[client-iplearn] [17062]: (info): MAC: 08be.ac3f IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
[client-auth] [17062]: (info): MAC: 08be.ac3f Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE
[client-iplearn] [17062]: (note): MAC: 08be.ac3f Client IP learn successful. Method: DHCP IP: 10.14.32.109
[client-iplearn] [17062]: (info): MAC: 08be.ac3f IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Received ip learn response. method: IPLEARN_METHOD_DHCP

Layer 3 authentication:

[client-orch-sm] [17062]: (debug): MAC: 08be.ac3f Triggered L3 authentication. status = 0x0, Success
[client-orch-state] [17062]: (note): MAC: 08be.ac3f Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
[client-auth] [17062]: (note): MAC: 08be.ac3f L3 Authentication initiated. LWA
[client-auth] [17062]: (info): MAC: 08be.ac3f Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]GET rcvd when in LOGIN state
[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]HTTP GET request
[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Parse GET, src [10.14.32.109] dst [10.107.221.82] url [http://firefox detect portal/]
[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Read complete: parse_request return 8
[webauth-io] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO state READING -> WRITING
[webauth-io] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO state WRITING -> READING
[webauth-io] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO state NEW -> READING
[webauth-io] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Read event, Message ready
[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]POST rcvd when in LOGIN state

Layer 3 authentication successful, move the client to the RUN state:

[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] Received User-Name guest for client 08be.ac3f
[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] auth mgr attr add/change notification is received for attr auth-domain(954)
[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] Method webauth changing state from 'Running' to 'Authc Success'
[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] Context changing state from 'Running' to 'Authc Success'
[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] auth mgr attr add/change notification is received for attr method(757)
[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] Raised event AUTHZ_SUCCESS (11)
[auth-mgr] [17062]: (info): [08be.ac3f:capwap_90000004] Context changing state from 'Authc Success' to 'Authz Success'
[webauth-acl] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Applying IPv4 logout ACL via SVM, name: IP-Adm-V4-LOGOUT-ACL, priority: 51, IIF-ID: 0
[webauth-sess] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Param-map used: global
[webauth-state] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Param-map used: global
[webauth-state] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]State AUTHC_SUCCESS -> AUTHZ
[webauth-page] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]Sending Webauth success page
[webauth-io] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO state AUTHENTICATING -> WRITING
[webauth-io] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO state WRITING -> END
[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 Remove IO ctx and close socket, id [99000029]
[client-auth] [17062]: (note): MAC: 08be.ac3f L3 Authentication Successful. ACL:[]
[client-auth] [17062]: (info): MAC: 08be.ac3f Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE
[webauth-httpd] [17062]: (info): capwap_90000004[08be.ac3f][10.48.39.243]56538/219 Remove IO ctx and close socket, id [D7000028]
[errmsg] [17062]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: Username entry (guest) joined with ssid (LWA_EA) for device with MAC: 08be.ac3f
[aaa-attr-inf] [17062]: (info): [Applied attribute :bsn-vlan-interface-name 0 " VLAN0039"]
[aaa-attr-inf] [17062]: (info): [Applied attribute : timeout 0 1800 (0x708)]
[aaa-attr-inf] [17062]: (info): [Applied attribute : url-redirect-acl 0 " IP-Adm-V4-LOGOUT-ACL"]
[ewlc-qos-client] [17062]: (info): MAC: 08be.ac3f Client QoS run state handler
[rog-proxy-capwap] [17062]: (debug): Managed client RUN state notification: 08be.ac3f
[client-orch-state] [17062]: (note): MAC: 08be.ac3f Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

Related Information

- **Cisco Technical Support & Downloads**